


# DCRS-7500 系列路由交换机

# 配置手册

神州数码(上海)网络有限公司

# 前言

DCRS-7500 交换机是神州数码网络有限公司设计制造的千兆多层交换机。为了帮助用户更好地了解、使用及日常维护 DCRS-7500 交换机，我们特编写了本手册。

# 第1章 产品介绍

## 1.1 产品简介

### 1.1.1 概述

DCRS-7504，DCRS-7508 和 DCRS-7515 系统是业界第一个能够使用一个产品系列向企业客户提供全面的端到端的 LAN 解决方案-从配线间，服务器池，数据中心到局域网主干的产品。新一代的 ASIC 芯片能够简化网络操作，管理以及设备备件，从而大大降低总的拥有成本（TCO）。

基于新一代的 ASIC 芯片组的神州数码 DCRS-7504，DCRS-7508 和 DCRS-7515 提供了无与伦比的端口密度，先进的第 2/3 层特性，丰富的服务质量（QoS）以及带宽管理能力，支持 10G 以太接口以扩展网络主干，提供高带宽容量。

### 1.1.2 产品特点

- 无与伦比的端口密度，在一个系统中可最多提供 672 个 10/100Base-TX 端口，232 个千兆以太网端口，232 个铜线千兆以太网端口，或者 14 个 10G 以太网端口；
- 丰富的 QoS 特性，提供线速细化带宽管理和全面的组播特性，为基于 IP 的语音传输（VoIP）和下一代流媒体应用打下了良好的基础；
- 先进的 2/3 层特性集，包括完全的 IP，IPX，AppleTalk 和 OSPF 协议支持；
- 基于策略的路由（PBR）；
- 提供每端口线速网络监视功能，可用于容量规划，故障查询和安全分析；
- 优异的高可用性，包括具有容余的，具有温度感应器的管理模块，可热插拔的负载均衡电源和可热插拔的接口模块；
- 能够防范拒绝服务（DoS）攻击和防止未经授权的网络和服务器组访问；
- 千兆和 10G 以太网接口上的 Jumbo 桢支持能力，便于提高网络主干吞吐率。

## 1.1.3 系统概览

表 1.1：系统概览

| 特性 | DCRS-7504 | DCRS-7508 | DCRS-7515 |
|---|---|---|---|
| 插槽数量 | 4 | 8 | 15 |
| 交换容量 | 128Gpbs | 256Gpbs | 480Gbps |
| 路由/交换速率（Mbps） | 48Mpps | 96Mpps | 178Mpps |
| 10/100 端口最大数量 | 144 | 336 | 672 |
| 千兆端口最大数量 | 56 | 120 | 232 |
| 10G 端口最大数量 | 3 | 7 | 14 |
| 高度 | 8.75 英寸(5RU) | 20.75 英寸(12RU) | 29.75 英寸(17RU) |
| 电源冗余 | 1+1 | N+1 | N+1 |

## 1.1.4 关键特性

### 1.1.4.1　优异的高可用性和高性能

- 冗余、可热插拔的管理和接口模块－快速故障检测和故障切换－提高系统的可靠性和可扩展性；
- 冗余、可热插拔的均衡电源－提高系统可靠性和电路冗余度，可在同一系统内混合使用交流的直流电源；
- 优异的第二层冗余 IEEE802.1w 的快速生成树协议(STP)和基于 IEEE803.ad 的链路聚合，能够实现快速收敛、最小化网络故障时间和最少的数据包丢失第三层冗余－VRRP、VRRPE（增强 VRRP）和 FSRP，实现路由器冗余；
- 业界最高的交换性能－非阻塞的分布式交换体系结构，采用一个并行交叉交换矩阵，提供高达 480Gpbs 的汇聚交换能力以及 178Mpps 的交换性能。

### 1.1.4.2　先进的第二层特性

- 丰富的生成树协议特性：
  - 快速生成树协议（IEEE802.1w）：亚秒级（50 毫秒－5 秒）收敛能力，使用一个预先计算好的备份链路；
  - 快速端口生成（Fast Port Span）：对于最终连接工作站的端口的端口实现更快的收敛，可在 4 秒内完成；

  - 快速上行链生成（Fast Uplink Span）：对于配线室内交换机上行链路端口实现 4 秒内的快速收敛；
  - 单实例 STP－根据 802.1s 技术规范，支持连接运行单一生成树实例的第三方设备；
  - PerVLAN STP(PVST)：单一系统内支持多个生成树，用于实现 VLAN 负载均衡，提高网络可靠性和性能。
- 动态 VLAN－根据端口、协议或子网，将用户逻辑划分到各个虚拟团体，从而简化网络地址管理，减少广播流量并确保网络安全；
- IEEE802.3ad 链路聚合－多达 4 个 100Mbps 或者 8 个千兆位以太网链路，可以聚合为一条平行的、负载均衡的链路，用于扩展网络带宽并防止物理链路、端口或接口模块故障；
- 镜像/监视端口－对单个或多个交换机端口进行监视和故障检测、不需要中断现有业务流，有助于故障隔离。

#### 1.1.4.3 完整的第三层功能

- 集成的交换路由（ISR）－减少了对外部路由器的依赖，允许网络管理员配置 DCRS-7500 交换机来实现三层路由，包括 IP、IPX、AppleTalk 以及 OSPF 协议；
- VRRP/VRRPE 和 FSRP－实现路由器冗余、用于提高网络可用性；
- 基于策略的路由（PBR）－基于源地址进行特定的客户化路由决策，允许企业客户为 VoIP 等关键业务提供增强的安全和可靠性，以及实现更有效的网络带宽利用；
- 网络地址转换 (NAT)－当需要穿越 Internet 网传输时，NAT 允许企业网络将专用 IP 地址转换为公用 IP 地址，从而保留 IP 地址空间，提高网络安全性。

#### 1.1.4.4 基础－先进的服务质量管理和带宽管理

- 先进的 QoS－根据端口、VLAN、源 MAC 地址、ACL、802.1p、服务类型（ToS）或 DiffServ 设置来执行或改变业务优先级，使关键业务流得到优先处理；
- 超低延迟－业界领先的 5 微秒端口到端口延迟、当使用 VoIP 时能实现优异的呼叫质量；
- 多种排队方法－严格的优先等级（SP）或加权公平排队（WFQ）能够灵活地实现业务优先等级划分；
- 线速、细化地带宽管理－基于端口、端口加优先级或第四层 ACL 的流量分类及带宽管理，动态速率限制设定从 256Kbps 到 1Gbps，以 256Kbps 为增量。

#### 1.1.4.5 可扩展组播实现方法

- 多种组播协议支持－IGMP、DVMRP、MSDP、PIM-SM（稀疏模式）以及 PIM-DM（密集模式），提供管理员很大的灵活性以支持不同的应用；
- 优异的组播可扩展性和性能－支持多达 64，000 个二层组播组以及亚秒级的加入和退出（join-and-leave）延迟时间，提供业界领先的组播性能和和扩展性。

#### 1.1.4.6 统一和易于使用的网络管理

- 全面的网络管理功能：致的完整的解决方案简化了网络管理操作和维护
  - Link Manager 网络管理软件：基于 SNMP 的集中式的图形界面，用于企业全网范围内的配置，维护和变更管理；
  - 命令行接口（CLI）：业界标准用户接口，最大程度降低了培训要求和操作维护成本；
  - Web 接口-所有神州数码网络产品采用标准的图形用户接口（GUI），易于使用，大大降低了安装时间和成本。
- SFlow（RFC3176）：每端口的线速网络流量监控提供了详细的流量统计，用于容量规划和实时网络监控，不影响网络性能。

#### 1.1.4.7 DCRS-7500 安全

- 线速扩展访问控制列表（ACL）：允许管理员控制数据包转发以及限制对系统管理接口的访问，同时提供线速数据交换和路由；
- 丰富的 ACL 实施方法：根据源或目的的 IP 地址，IP 协议类型，TCP 或 UDP 端口，IP 优先次序或服务类型值等来识别数据流；
- 选择性 ACL 记录：收集符合拒绝或许可条件的数据包的统计数据；
- 方便管理：根据名称或数字来标记 ACL，或添加一行注释文字；
- ACL 语法兼容性：所有神州数码网络产品采用统一的 ACL 语法，并与其他主要厂商语法兼容；
- Secure Shell 和 Secure Copy：通过网络安全地访问管理接口；
- 防范拒绝服务（DoS）攻击：通过限制 TCP SYN 和 ICMP 数据包，防止恶意用户攻击，尽量减少网络故障时间；通过限制广播数据包，防止广播风暴；
- 用户认证-支持 AAA，802.1x，RADIUS，TACACS 和 TACACS+认证，防止未经授权的网络访问。

## 1.2 产品外观

神州数码 DCRS-7500 交换机提供了 3 种机箱规格（见图 1.1）：

- DCRS-7515
- DCRS-7508
- DCRS-7504

图 1.1 ：DCRS-7500 交换机的 3 种机箱规格



DCRS-7515　　DCRS-7508　　DCRS-7504

其中 DCRS-7515 提供了 15 个插槽；DCRS-7508 提供了 8 个插槽；DCRS-7504 提供了 4 个插槽；每个插槽中可以插入管理模块（Management Module）或转发模块（Forwarding Module）。神州数码 DCRS-7500 交换机支持冗余管理模块，用户可以安装配置第二个管理模块提供冗余（详见第二章）。

表 1.2 列出了 DCRS-7500 系列路由交换机所支持的模块。

表 1.2：DCRS-7500 系列路由交换机标准模块列表

| MRS-7500-M2GS | 标准 DCRS-7500 系列三层管理模块，含 2 口 1000Base-SX 千兆光纤接口（SC 接口）,支持静态路由 |
|---|---|
| MRS-7500-M4GS | 标准 DCRS-7500 系列三层管理模块，含 4 口 1000Base-SX 千兆光纤接口（SC 接口）,支持静态路由 |
| MRS-7500-M8GS | 标准 DCRS-7500 系列三层管理模块，含 8 口 1000Base-SX 千兆光纤接口（SC 接口）,支持静态路由 |
| MRS-7500-M2GL | 标准 DCRS-7500 系列三层管理模块，含 2 口 1000Base-LX 千兆光纤接口（SC 接口）,支持静态路由 |
| MRS-7500-M4GL | 标准 DCRS-7500 系列三层管理模块，含 4 口 1000Base-LX 千兆光纤接口（SC 接口）,支持静态路由 |
| MRS-7500-8GS | 标准 DCRS-7500 系列 8 口 1000Base-SX 千兆光纤模块（SC 接口） |
| MRS-7500-8GL | 标准 DCRS-7500 系列 8 口 1000Base-LX 千兆光纤模块（SC 接口） |
| MRS-7500-8GT | 标准 DCRS-7500 系列 8 口 100/1000Base-T 模块 |
| MRS-7500-24TX | 标准 DCRS-7500 系列 24 口 10/100 Base-TX 模块 |
| MRS-7500-24FX | 标准 DCRS-7500 系列 24 口 100Base-FX 百兆多模光纤模块 （MT-RJ 接口） |
| MRS-7500-24FL | 标准 DCRS-7500 系列 24 口 100Base-FX 百兆单模光纤模块 （MT-RJ 接口）,支持 15 公里传输距离 |
| ULH-7500-70 | 1000Base-SX—1000Base-LH70 端口升级，此为每 SX 端口升级报价，需在订货时注明升级模块型号、数量以及每个模块升级端口数量。LH70，最小衰减 10db，9 或 10μm 单模光纤≤70km（适用于 DCRS-7500） |
| ULH-7500-150 | 1000Base-SX—1000Base-LH150 端口升级，此为每 SX 端口升级报价，需在订货时注明升级模块型号、数量以及每个模块升级端口数量。LH150，最小衰减 10db，9 或 10μm 单模光纤≤150km（适用于 DCRS-7500） |

# 第2章 交换机的管理

用户可以通过下面方式管理交换机：

- 命令行界面（Command Line Interface）：通过直连串口或 Telnet 连接管理交换机的字符界面。
- Web 管理界面（Web management interface）：通过 HTTP（Web 浏览）连接管理交换机的图形用户界面（GUI）

## 2.1 命令行界面（CLI）

通常用户会在首次配置交换机时使用命令行界面。使用命令行界面时，按下列过程操作：

1. 将 1 台 PC 用直通线（straight-through cable）连接到串口上，串口有 DB-9 的公头；
2. 直通线的另一端连接到交换机管理模块的 Console 口上
3. 在 PC 机上运行终端仿真程序，设置串口为以下参数：

   Baud: 9600 bps
   Data bits: 8
   Parity: None
   Stop bits: 1
   Flow control: None
   按“回车键”，即可进入配置界面：
   DCRS-7500>

在 CLI 下，系统命令分 3 种配置模式：

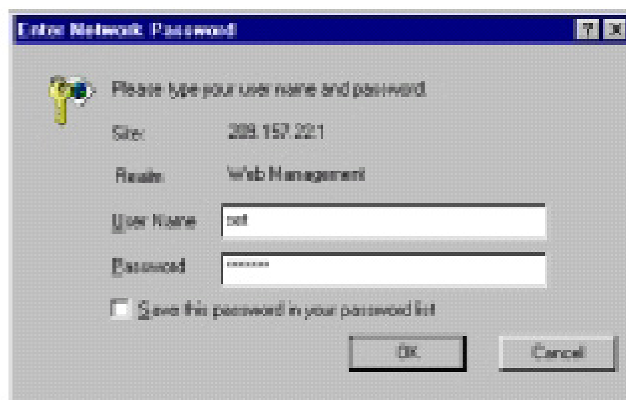
- 用户配置模式（User EXEC）：可以显示一些信息和进行基本的命令如 ping 和 traceroutes；
- 特权配置模式（Privileged EXEC）：除了可以使用所有用户配置模式的命令外，还可以使用不需要将改变保存与 system-config 文件的配置命令；
- 全局配置模式（CONFIG）：允许用户对整个交换机进行配置。为了使能够使交换机在重启后保存配置改变，需要将配置保存在 system-config 文件中。全局配置模式包括一些子模式，例如端口配置模式，VLAN 配置模式，路由配置模式等。

## 2.2 Web 管理界面

使用 Web 管理界面，需要打开 Web 浏览器，输入交换机的 IP 地址。Web 浏览器联系交换机，显示出交换机的对话框。

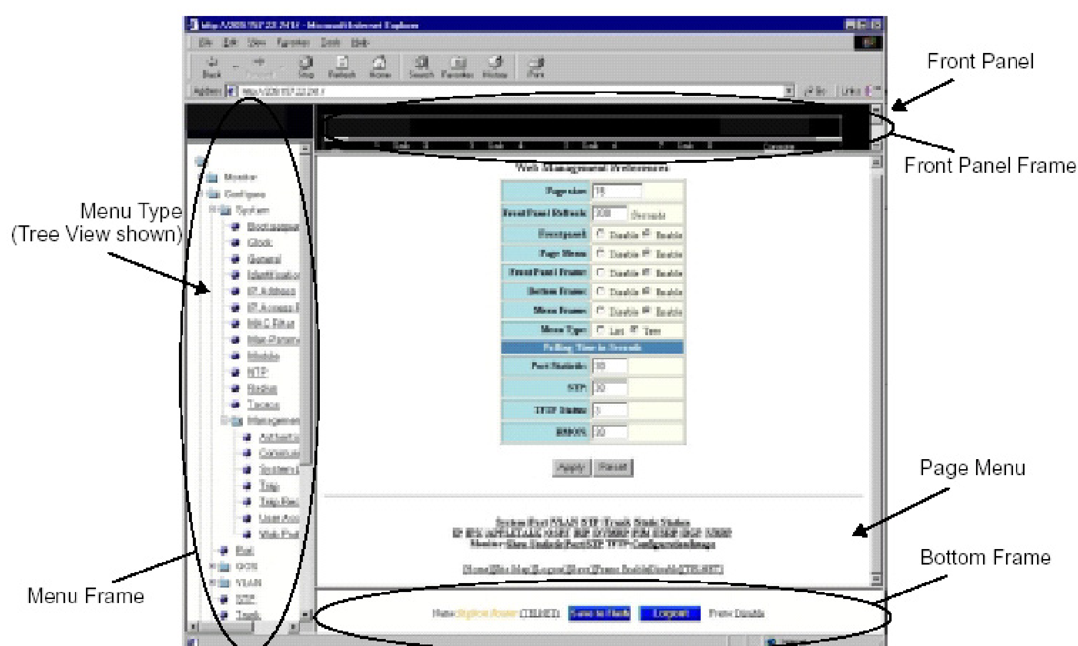
要想登陆，点击 Login，会显示出下面对话框。

图 2.1：Web 管理界面登陆对话框




用户输入用户名（user name）和密码（password）登陆，交换机会显示出如下图所示的配置界面。用户可以点击相应的链接对交换机进行配置。

图 2.2：Web 管理界面



# 第3章 基本配置

这一章介绍如何使用 CLI（Command Line Interface）配置基本的，非协议相关的一些参数，包括：

- 基本系统参数
- 基本端口参数
- 基本二层参数
- 基本三层参数
- 系统默认参数
- 温度感应参数
- 端口镜像

神州数码交换机在出厂时已经进进行了默认配置，但许多高级特性，比如 VLANs 和路由协议等必须在全局配置模式（Global CONFIG）下手工进行配置。

## 3.1 配置基本系统参数

### 3.1.1 输入系统管理信息

用户可以在神州数码 DCRS-7500 交换机上配置系统名字，地址或联系方式作为参考，这些信息存储在本地的配置文件中。当用户配置了系统名字，这个名字将替代原来的 CLI 提示符。系统名字，地址或联系方式可以是 32 位的字母或数字。

**命令：** **hostname <string>**
**功能：** 定义系统名字
**命令模式：** 全局配置模式
**使用指南：** 当名字中含有空格时，需要使用引号
**举例：**

```
DCRS-7500(config)# hostname zappa
zappa(config)# end
zappa# write memory
```

### 3.1.2 配置 Simple Network Management (SNMP) 参数

#### 3.1.2.1 指定 SNMP Trap 接受主机

用户可以为交换机发出的所有 SNMP traps 指定一个接受主机。当指定接受主机时可以同时指定 community string。交换机发出所有 SNMP traps 时，同时发出 community string。这

样系统管理员能够根据 IP 地址和 community string 来过滤 traps 是从那一台交换机发出的。

当用户指定 Trap 接受主机时，在 CLI 或 Web 管理界面显示 community string 时，系统软件自动对 string 进行加密。如果用户希望在显示时看到 string 的明文，可以在指定 SNMP Trap 接受主机时做相应配置。

命令： snmp-server host <ip-addr> [0 | 1] <string>

功能： 指定 SNMP Trap 接受主机

命令模式： 特权配置模式

参数： <ip-addr>指定 SNMP Trap 接受主机的 IP 地址；0 | 1 中 0 指明文 string，1 指密文 string，默认状态是 0；<string>的作用是是接受主机容易识别 SNMP Trap 是从哪一台设备发出的。

举例：

```
DCRS-7500(config)# snmp-server host 2.2.2.2 0 DCRS-7500-12
DCRS-7500(config)# write memory
```

上述命令指定主机 2.2.2.2 接受交换机发出的 SNMP traps，并使用明文显示 string。

#### 3.1.2.2 指定单一 Trap 源地址

用户可以为所有交换机发出的 SNMP traps 指定单一的源 IP 地址。用户可以指定以太端口，loopback 接口或虚拟接口（virtual interface），交换机会使用这些端口或接口的首个 IP 地址作为交换机所有 Trap 的源 IP 地址。

指定单一 Trap 源地址有如下好处：

- 简化 SNMP Trap 接受主机的设置。接受主机只需配置交换机的单一 Trap 源地址，即可接受全部由交换机发出的 SNMP traps；
- 如果用户指定 loopback 地址作为单一 Trap 源地址，那么当交换机的个别端口 Down 时，接受主机仍能通过其他端口接受到 SNMP traps。

命令： snmp-server trap-source loopback <num> | ethernet <portnum> | ve <num>

功能： 指定单一 Trap 源地址

命令模式： 特权配置模式

参数： loopback <num>设定 loopback 接口<num>为单一 Trap 源地址；ethernet <portnum>设定以太端口<portnum>为单一 Trap 源地址；ve <num>设定虚拟接口<num>为单一 Trap 源地址

举例一：

```
DCRS-7500(config)# snmp trap-source ethernet 4/11
DCRS-7500(config)# write memory
```

上述命令指定交换机发出的所有 SNMP Trap 都以以太端口 4/11 为源地址。

举例二：

```
DCRS-7500(config)# int loopback 1
DCRS-7500(config-lbif-1)# ip address 10.0.0.1/24
DCRS-7500(config-lbif-1)# exit
DCRS-7500(config)# snmp-server trap-source loopback 1
```

上述命令指定交换机发出的所有 SNMP Trap 都以 lookback 1 为源地址。

### 3.1.3 配置端口为所有 Telnet 包的源地址

用户可以指定 1 个端口的最小 IP 地址为三层交换机的所有 Telnet 包的源地址。这样做会带来如下好处：

- 当 Telnet 服务器配置了只接受特定的 IP 地址发来的 Telnet 包时，这样配置可以简化 Telnet 服务器的配置工作。Telnet 服务器只需配置 1 个交换机的 Telnet 地址即可接受从交换机发出的所有 Telnet 包。
- 如果用户指定 loopback 地址作为所有 Telnet 包的源地址，那么当交换机的个别端口 Down 时，Telnet 服务器仍能接受其他端口发送的 Telnet 包，并认为是从同一源地址发出的。

命令： ip telnet source-interface ethernet <portnum> | loopback <num> | ve <num>
功能： 配置端口为所有 Telnet 包的源地址
命令模式： 全局配置模式
参数： loopback <num>设定 loopback 接口<num>为所有 Telnet 包的源地址；ethernet <portnum>设定以太端口<portnum>为所有 Telnet 包的源地址；ve <num>设定虚拟接口<num>为所有 Telnet 包的源地址
使用指南： 系统自动将端口最小的 IP 地址设置成所有 Telnet 包的源地址
举例一：

```
DCRS-7500(config)# int loopback 2
DCRS-7500(config-lbif-2)# ip address 10.0.0.2/24
DCRS-7500(config-lbif-2)# exit
DCRS-7500(config)# ip telnet source-interface loopback 2
```

上述命令指定交换机发出的所有 Telnet 包都以以 Lookback 2 为源地址。

举例二：

```
DCRS-7500(config)# interface ethernet 1/4
DCRS-7500(config-if-1/4)# ip address 209.157.22.110/24
DCRS-7500(config-if-1/4)# exit
DCRS-7500(config)# ip telnet source-interface ethernet 1/4
```

上述命令指定交换机发出的所有 Telnet 包都以以太端口 4/11 为源地址。

### 3.1.4 配置端口为所有 TFTP 包的源地址

用户可以指定 1 个端口的最小 IP 地址为三层交换机的所有 TFTP 包的源地址。

命令： [no] ip tftp source-interface ethernet <portnum> | loopback <num> | ve <num>
功能： 配置端口为所有 TFTP 包的源地址
命令模式： 全局配置模式

参数：　loopback <num>设定 loopback 接口<num>为所有 TFTP 包的源地址；ethernet <portnum>设定以太端口<portnum>为所有 TFTP 包的源地址；ve <num>设定虚拟接口<num>为所有 TFTP 包的源地址

使用指南：　系统自动将端口最小的 IP 地址设置成所有 Telnet 包的源地址

举例：

```
DCRS-7500(config)# int ve 1
DCRS-7500(config-vif-1)# ip address 10.0.0.3/24
DCRS-7500(config-vif-1)# exit
DCRS-7500(config)# ip tftp source-interface ve 1
```

上述命令指定交换机发出的所有 TFTP 包都以以虚拟地址 1 为源地址。

### 3.1.5 改变千兆协商模式

用户可以将默认千兆协商模式配置成以下模式中的一种：

- Negotiate-full-auto：端口首先试图与另一端端口进行握手来交换端口性能信息。如果另一端没有应答，端口使用手工配置的配置信息（如果系统管理员没有配置，则使用默认配置）。这种模式是系统默认的模式。
- Auto-Gigabit：端口试图与另一端端口进行握手来交换端口性能信息。
- Negotiation-off：端口不与另一端进行握手，而是使用手工配置的配置信息。

传统的千兆端口必须两端同时配置成相同的模式（Auto-Gigabit 或 Negotiation-off）时，才能建立连接。神州数码 DCRS-7500 交换机提供了新的千兆协商模式，当千兆接口配置成 Negotiate-full-auto 时，端口会先用 Auto-Gigabit 模式与对端端口协商，如果协商失败在切换到 Negotiation-off 模式。

命令：　gig-default neg-full-auto | auto-gig | neg-off

功能：　改变千兆协商模式

命令模式：　全局配置模式或端口配置模式

举例一：

```
DCRS-7500(config)# gig-default neg-off
```

上面命令把所有千兆端口都配置成 Negotiation-off 模式，但不包括在端口配置模式下配置了其他协商模式的端口。

举例二：

```
DCRS-7500(config)# int ethernet 4/1 to 4/4
DCRS-7500(config-mif-4/1-4/4)# gig-default auto-gig
```

上述命令把端口 4/1 到 4/4 的端口千兆协商模式重新定义为 Auto-Gigabit。

### 3.1.6 限制广播，组播或单播速率

神州数码 DCRS-7500 交换机可以将所有流量以线速转发，但是一些其他交换机无法处

理高速转发流量。用户可以限制每秒交换机转发的广播，组播或单播数据包的数量。

#### 3.1.6.1 限制广播速率

命令： broadcast limit <num>
功能： 每秒最多转发数据包的广播数据包的数量
命令模式： 全局配置模式或端口配置模式
参数： <num>表示每秒最多转发数据包的广播数据包的数量
举例一：

```
DCRS-7500(config)# broadcast limit 100000
DCRS-7500(config)# write memory
```

上述命令将交换机每秒转发广播数据包的数量限制在 100000 个。

举例二：

```
DCRS-7500(config)# int ethernet 1/3
DCRS-7500(config-if-1/3)# broadcast limit 80000
DCRS-7500(config-if-1/3)# write memory
```

上述命令将交换机端口 1/3 每秒转发广播数据包的数量限制在 80000 个。

#### 3.1.6.2 限制组播速率

命令： multicast limit <num>
功能： 每秒最多转发数据包的组播数据包的数量
命令模式： 全局配置模式或端口配置模式
参数： <num>表示每秒最多转发数据包的组播数据包的数量
举例一：

```
DCRS-7500(config)# multicast limit 120000
DCRS-7500(config)# write memory
```

上述命令将交换机每秒转发组播数据包的数量限制在 120000 个。

举例二：

```
DCRS-7500(config)# int ethernet 3/6
DCRS-7500(config-if-3/6)# multicast limit 55000
DCRS-7500(config-if-3/6)# write memory
```

上述命令将交换机端口 3/6 每秒转发组播数据包的数量限制在 55000 个。

#### 3.1.6.3 限制单播速率

命令： unknown-unicast limit <num>
功能： 每秒最多转发数据包的单播数据包的数量

命令模式：　全局配置模式或端口配置模式
参数：　　　<num>表示每秒最多转发数据包的单播数据包的数量
举例一：
```
DCRS-7500(config)# unknown-unicast limit 110000
DCRS-7500(config)# write memory
```
上述命令将交换机每秒转发单播数据包的数量限制在 110000 个。

举例二：
```
DCRS-7500(config)# int ethernet 4/2
DCRS-7500(config-if-4/2)# unknown-unicast limit 40000
DCRS-7500(config-if-4/2)# write memory
```
上述命令将交换机端口 2/4 每秒转发单播数据包的数量限制在 40000 个。

## 3.2 配置基本端口参数

神州数码 DCRS-7500 交换机预先对所有端口进行了初始配置，开机后可直接使用。也可以改变端口参数配置以适应不同的网络需要。

### 3.2.1 给端口分配名称

端口名称用来在网络中识别端口，可以分配给物理端口，虚拟接口和 loopback 接口。

命令：　　　port-name <text>
功能：　　　给端口分配名称
命令模式：　端口配置模式
参数：　　　<text>表示端口名称，名称可以时字母或数字，最多 255 个字符。名称中可以包括空格，包括空格时无需引号。
举例：
```
DCRS-7500(config)# interface e 2/8
DCRS-7500(config-if-2/8)# port-name Marsha the Marketing Monkey
```
上述命令将端口 2/8 命名为 Marsha the Marketing Monkey

### 3.2.2 改变端口速率

所有的 10BaseT/100BaseTX 端口都与相连的设备自适应自协商速率和模式。如果相连设备不支持自适应，自协商速率和模式，可以手工在交换机上配置相应参数。10BaseT/100BaseTX 端口的默认时 10/100 自适应。

100BaseFX 端口总是工作在 100 Mbps 全双工模式下，不可改变。

1000BaseSX, 1000BaseLX, 1000BaseT, and 1000BaseLH 端口总是工作在 1000 Mbps 全双工模式下，不可改变。

命令： speed-duplex <value>
功能： 改变端口速率
命令模式： 端口配置模式
参数： <value>可取的值为：10-full；10-half；100-full；100-half；auto。默认值时 auto
举例：

```
DCRS-7500(config)# interface e8
DCRS-7500(config-if-8)# speed-duplex 10-full
```

上述命令把端口 8 的速率设定为 10Mbps。

### 3.2.3 改变端口模式

用户可以把端口设置成全双工（full-duplex）和半双工（half-duplex）。这个选项只在 10/100 Mbps 端口上支持。The 100BaseFx, 1000BaseSx 和 1000BaseLx 端口只支持全双工。

命令： speed-duplex <value>
功能： 改变端口模式
命令模式： 端口配置模式
参数： <value>可取的值为：10-full；10-half；100-full；100-half；auto。默认值时 auto
举例：

```
DCRS-7500(config)# interface e8
DCRS-7500(config-if-8)# speed-duplex 10-full
```

上述命令把端口 8 的模式设定为全双工。

### 3.2.4 开启和停止端口

命令： enable/disable
功能： 开启和停止端口
命令模式： 端口配置模式
举例一：

```
DCRS-7500(config)# interface e 1/8
DCRS-7500(config-if-1/8)# disable
```

上述命令停止端口 1/8。

举例二：

```
DCRS-7500(config)# interface ve v1
DCRS-7500(config-vif-1)# enable
```

上述命令开启虚拟接口 1。

### 3.2.5 开启和停止流量控制（Flow Control）

用户可以在全双工端口上开启和停止流量控制（802.3x）功能。默认状态下，流量控制功能开启。

命令：　　　[no] flow-control
功能：　　　开启和停止流量控制
命令模式：　全局配置模式
举例一：

```
DCRS-7500(config)# no flow-control
```

上述命令停止流量控制功能。

举例二：

```
DCRS-7500(config)# flow-control
```

上述命令开启流量控制功能。

## 3.3 配置基本二层参数

### 3.3.1 开启和停止生成树协议（Spanning Tree Protocol）

神州数码 DCRS-7500 交换机支持生成树协议（IEEE 802.1d bridge protocol）。该协议通过特定的算法在交换机网络中阻断部分冗余路径，建立起无环路的树状网络，以避免网络无限循环。

STP 必须在全局模式开启才能够在 VLAN 模式支持此功能。在二层交换机上，STP 默认开启；在三层交换机上，STP 默认停止。

命令：　　　[no] spanning-tree
功能：　　　开启和停止生成树协议
命令模式：　全局配置模式
举例一：

```
DCRS-7500(config)# spanning tree
```

上述命令在全局开启 STP。

### 3.3.2 开启和停止二层交换（三层交换机功能）

默认状态下，神州数码 DCRS-7500　三层交换机支持二层交换。对于交换机不支持的

路由协议，交换机交换这些路由协议。用户可以全局或基于端口停止二层交换功能。

命令：　[no] route-only
功能：　开启和停止二层交换
命令模式：　全局命令模式或端口命令模式
举例一：

```
DCRS-7500(config)# route-only
DCRS-7500(config)# exit
DCRS-7500# write memory
DCRS-7500# reload
```

上述命令停止三层交换机上的二层交换功能。

举例二：

```
DCRS-7500(config)# interface ethernet 3/2
DCRS-7500(config-if-3/2)# route-only
```

上述命令停止端口 3/2 上的二层交换功能。

### 3.3.3 改变 MAC 的老化时间

这个参数定义了 1 个端口的 MAC 地址在地址表中保存的时间。它的取值范围是 0 或者从 67 到 65539 秒。0 代表 MAC 地址永不老化。默认值为 300（秒）。

命令：　[no] mac-age-time <age-time>
功能：　改变 MAC 的老化时间
命令模式：　全局配置模式
参数：　<age-time>取值范围是 0 或者从 67 到 65539，默认值为 300。
举例：

```
DCRS-7500(config)# mac-age-time 600
```

上面命令把交换机的 MAC 的老化时间设定为 600 秒。

### 3.3.4 端口地址数量限制

端口地址数量限制使用户能够限制可以访问端口设备的数量。非法访问会被作为 SNMP traps 发送。这项功能默认状态下关闭。端口的最大地址条目数量使 2048 个，默认使 8 个。

命令：　lock-address ethernet <portnum> [addr-count <num>]
功能：　限制端口地址数量
命令模式：　全局配置模式
参数：　<portnum>表示以太网端口号；<num>表示最大端口地址数量。
举例：

```
DCRS-7500(config)# lock e 2 addr 15
```

上述命令将端口 2 的最大地址数量设置为 15。

# 3.4 配置基本三层参数

## 3.4.1 开启的关闭路由协议

神州数码 DCRS-7500 交换机支持下列路由协议：

- AppleTalk
- DVMRP
- FSRP
- IP
- IPX
- OSPF
- PIM
- RIP
- VRRP
- VRRPE

默认状态下，三层交换机的 IP 路由是开启的，其他路由协议都是关闭的，需要用户开启和配置才能使用。

**命令：** router appletalk | bgp | dvmrp | fsrp | ipx | ospf | pim | rip | vrrp | vrrpe
**功能：** 开启路由协议
**命令模式：** 全局配置模式
**参数：** appletalk | bgp | dvmrp | fsrp | ipx | ospf | pim | rip | vrrp | vrrpe 表示需要开启的路由协议
**举例：**

```
DCRS-7500(config)# router ospf
DCRS-7500(config)# end
DCRS-7500# write memory
DCRS-7500# reload
```

上述命令将开启 ospf 路由协议。

## 3.4.2 显示和修改系统参数

神州数码 DCRS-7500 交换机对于下列参数有相应的默认表单大小。表单大小决定了表单中最多可以容纳的条目数量。用户可以改变表单大小以适应配置需要。

- MAC address entries
- Layer 2 Port VLANs supported on a system
- Layer 3 Protocol VLANs supported on a system

- Layer 4 sessions supported
- IP cache size
- ARP entries
- IP routes
- IP route filters
- IP sub-nets per port and per device
- Static routes
- IGMP
- DVMRP routes
- IPX/SAP entries
- IPX/RIP entries
- IPX/SAP filters
- IPX/RIP filters
- IPX forwarding filters
- AppleTalk routes

命令： show default values
功能： 显示系统参数
命令模式： 特权配置模式
举例：

```
DCRS-7500# show default values

sys log buffers:50     mac age time:300 sec      telnet sessions:5

ip arp age:10 min      bootp relay max hops:4    ip ttl:64 hops
ip addr per intf:24

when multicast enabled :
igmp group memb.:140   sec igmp query:60 sec

when ospf enabled :
ospf dead:40 sec       ospf hello:10 sec         ospf retrans:5 sec
ospf transit delay:1 sec

when bgp enabled :
bgp local pref.:100    bgp keep alive:60 sec     bgp hold:180 sec
bgp metric:10          bgp local as:1            bgp cluster id:0
bgp ext. distance:20   bgp int. distance:200     bgp local distance:200

System Parameters      Default     Maximum     Current
ip-arp                 8000        64000           8000
ip-static-arp          1024        2048            1024
atalk-route            512         1536            512
atalk-zone-port        64          255             64
```

| | | | |
|---|---|---|---|
| atalk-zone-sys | 255 | 1024 | 255 |
| dvmrp | 2048 | 32000 | 2048 |
| igmp | 256 | 1024 | 256 |
| ip-cache | 128000 | 256000 | 128000 |
| ip-filter-port | 512 | 4096 | 512 |
| ip-filter-sys | 1024 | 8192 | 1024 |
| ipx-forward-filter | 256 | 1024 | 256 |
| ipx-rip-entry | 3072 | 32728 | 3072 |
| ipx-rip-filter | 256 | 1024 | 256 |
| ipx-sap-entry | 6144 | 32768 | 6144 |
| ipx-sap-filter | 256 | 1024 | 256 |
| l3-vlan | 32 | 2048 | 32 |
| ip-qos-session | 2048 | 32000 | 2048 |
| l4-real-server | 1024 | 2048 | 1024 |
| l4-virtual-server | 256 | 512 | 256 |
| l4-server-port | 2048 | 4096 | 2048 |
| mac | 8000 | 64000 | 8000 |
| ip-route | 128000 | 200000 | 128000 |
| ip-static-route | 512 | 2048 | 512 |
| vlan | 16 | 2048 | 16 |
| spanning-tree | 32 | 128 | 32 |
| mac-filter-port | 32 | 512 | 32 |
| mac-filter-sys | 64 | 1024 | 64 |
| ip-subnet-port | 24 | 128 | 24 |
| session-limit | 131072 | 500000 | 131072 |
| view | 10 | 65535 | 10 |
| virtual-interface | 255 | 2048 | 255 |

**命令：** system-max ip-route <num>
**功能：** 改变系统 IP 路由表大小
**命令模式：** 特权配置模式
**参数：** <num>表示 IP 路由表最大条目数量
**使用指南：** 修改配置后，需要保存并重启交换机使配置生效。
**举例：**

```
DCRS-7500(config)# system-max ip-route 120000
DCRS-7500(config)# write memory
DCRS-7500(config)# exit
DCRS-7500# reload
```

上述命令把系统 IP 路由表大小设置为最大 120000 条目。

**命令：** system-max subnet-per-interface <num>
**功能：** 改变每端口最大子网数

命令模式： 特权配置模式
参数： <num>表示每端口最大子网数
使用指南： 修改配置后，需要保存并重启交换机使配置生效。
举例：

```
DCRS-7500(config)# system-max subnet-per-interface 64
DCRS-7500(config)# write memory
DCRS-7500(config)# exit
DCRS-7500# reload
```

命令： system-max subnet-per-system <num>
功能： 改变系统最大子网数
命令模式： 特权配置模式
参数： <num>表示系统最大子网数
使用指南： 修改配置后，需要保存并重启交换机使配置生效。
举例：

```
DCRS-7500(config)# system-max subnet-per-system 512
DCRS-7500(config)# write memory
DCRS-7500(config)# exit
DCRS-7500# reload
```

## 3.5 使用温度感应

温度感应功能使模块温度在超过一定警告级别（warning level）或关机级别（shutdown level）时生成日志文件（Syslog message）和SNMP trap，并在温度超过安全阀值时停止模块运行。

用户可以显示和改变温度的警告级别和关机级别。系统软件根据交换机的轮询时间（poll time）来读取温度感应。默认轮询时间时60秒。

当温度连续达到和超过关机级别5次，系统软件会停止模块运行以防止烧毁模块。用户可以显示当时温度并可以改变系统轮询时间。

### 3.5.1 显示模块温度

系统软件按照轮询时间读取温度，默认状态下是60秒。轮询时间还决定了系统软件读取其他系统参数的时间间隔。

命令： show chassis
功能： 显示模块温度
命令模式： 用户配置模式
举例：

```
DCRS-7500> show chassis
power supply 1 not present
```

```
power supply 2 not present
power supply 3 ok
power supply 4 not present
power supply 1 to 4 from bottom to top
fan 1 ok
fan 2 bad
fan 3 ok
fan 4 ok
Current temperature : 34.5 C degrees
Warning level : 45 C degrees, shutdown level : 55 C degrees
```

### 3.5.2 改变温度的警告级别和关机级别

默认的温度警告级别是 45.0 度；默认的温度警告级别是 55.0 度。用户可以改变温度的警告级别和关机级别，取值范围是从 0 到 125 度。

命令： temperature warning <value>
功能： 改变温度的警告级别
命令模式： 特权配置模式
参数： <value>表示警告级别的温度
举例：

```
DCRS-7500# temperature warning 47
```

上述命令把警告级别的温度定位 47 度。

命令： temperature shutdown <value>
功能： 改变温度的关机级别
命令模式： 特权配置模式
参数： <value>表示关机级别的温度
举例：

```
DCRS-7500# temperature shutdown 57
```

上述命令把关机级别的温度定位 57 度。

### 3.5.3 改变交换机的轮询时间

系统软件按照轮询时间读取温度，默认状态下是 60 秒。

命令： chassis poll-time <value>
功能： 改变交换机的轮询时间
命令模式： 特权配置模式
参数： <value>轮询时间，单位是秒

举例：

```
DCRS-7500(config)# chassis poll-time 200
```

上述命令将交换机的轮询时间设定为 200 秒。

## 3.6 配置端口镜像

在 DSRS-7500 交换机上，用户可以配置另外一个端口来“镜像”想监视的端口，然后通过在这个镜像端口外接协议分析仪来查看被镜像端口的流量信息。

在一个端口上做端口镜像需要两个步骤：

- 激活一个端口作为镜像端口，这个端口连接协议分析仪
- 激活被镜像的端口的镜像功能

用户可以监视输入流量、输出流量或者双向流量。任何一个端口都可以作为镜像端口，可以配置最多 64 个镜像端口。不同的模块上都可以配置镜像端口，也可以在同一模块上配置多个镜像端口。

每一个镜像端口都有自己的被镜像端口。镜像和被镜像端口可以在不同模块上。

### 3.6.1 配置端口镜像

命令： [no] mirror-port ethernet <portnum>
功能： 激活镜像端口
命令模式： 特权配置模式
参数： <portnum>为镜像端口的端口号

命令： [no] monitor ethernet <portnum> [ethernet <portnum>...] both | in | out
功能： 激活被镜像的端口的镜像功能
命令模式： 端口配置模式
参数： <portnum>为镜像端口端口号；both | in | out 分别代表双向流量，输入流量，输出流量

举例一：

```
DCRS-7500(config)# mirror-port ethernet 4/1
DCRS-7500(config)# interface ethernet 4/3
DCRS-7500(config-if-4/3)# monitor ethernet 4/1 both
```

上述命令将端口 4/3 上的双向流量镜像到端口 4/1，用户可以在端口 4/1 外接协议分析仪来查看端口 4/3 的流量信息。

举例二：

```
DCRS-7500(config)# interface ethernet 1/2
DCRS-7500(config-if-1/2)# monitor ethernet 1/1 in
```

```
DCRS-7500(config-if-1/2)# interface ethernet 1/3
DCRS-7500(config-if-1/3)# monitor ethernet 1/1 in
DCRS-7500(config-if-1/3)# interface ethernet 1/4
DCRS-7500(config-if-1/4)# monitor ethernet 1/1 in
```

上述命令把端口 1/2，1/3 和 1/4 的输入流量镜像到端口 1/1。

### 3.6.2 镜像链路聚合组中的单独端口

默认状态下，当镜像链路聚合组中的主端口时，链路聚合组中的所有端口的流量都被镜像到镜像端口。用户可以配置只镜像链路聚合组中的单独端口。

命令： [no] monitor ethe-port-monitored <portnum> | named-port-monitored <portname> ethernet <portnum> in | out | both
功能： 镜像链路聚合组中的单独端口
命令模式： 链路聚合配置模式
参数： ethe-port-monitored <portnum> | named-port-monitored <portname>参数指定了链路聚合组中被镜像的端口，ethe-port-monitored <portnum>指定被镜像的端口号码，named-portmonitored <portname>指定被镜像的端口名称；ethernet | <portnum>指定镜像端口号码，这个端口外接协议分析仪；both | in | out 分别代表双向流量，输入流量，输出流量
举例：

```
DCRS-7500(config)# mirror ethernet 2/1
DCRS-7500(config)# trunk switch ethernet 4/1 to 4/8
DCRS-7500(config-trunk-4/1-4/8)# monitor ethe-port-monitored 4/5 ethernet 2/1
in
```

上述命令设置端口 2/1 镜像链路聚合组中端口 4/5 的输入流量。

命令： [no] config-primary-ind
功能： 镜像链路聚合组中的主端口
命令模式： 链路聚合配置模式
举例：

```
DCRS-7500(config)# mirror ethernet 2/1
DCRS-7500(config)# trunk switch ethernet 4/1 to 4/8
DCRS-7500(config-trunk-4/1-4/8)# config-primary-ind
DCRS-7500(config-trunk-4/1-4/8)# monitor ethe-port-monitored 4/1 ethernet 2/1
out
```

上述命令设置端口 2/1 镜像链路聚合组中主端口 4/1 的输出流量。

### 3.6.3 显示端口镜像配置

命令： show monitor

**功能：** 显示端口镜像配置

**命令模式：** 全局配置模式

**举例：**

```
DCRS-7500(config)# show monitor
Mirror Interface:      ethernet 4/1
Monitored Interfaces:
    Both            Input       Output
    ---------------------------------------------------
    ethernet 4/3
```

# 第4章 配置 Span Tree Protocol（STP）

## 4.1 STP 简介

STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议通过特定的算法在交换机网络中阻断部分冗余路径，建立起无环路的树状网络，以避免网络无限循环。

STP 的基本原理是，通过网桥之间传递较小的信息包——网桥协议数据单元 BPDU（Bridge Protocol Data Unit），来决定阻塞那些冗余链路端口，从而建立起树状网络结构。网桥协议数据单元 BPDU 是周期发送的，网桥接收到 BPDU 后，利用 STA 算法（Spanning Tree Algorithm，即生成树算法）进行计算，判断出网络上是否存在循环，如果存在循环则做出阻塞冗余端口的决定。被阻塞的端口不能接收和转发数据流量，但仍然是一个活动的端口，可以接收和读取 BPDU。一旦网络拓扑发生变化，网桥利用 STA 算法，重新决定转发端口和阻塞端口，原先的阻塞端口可能就成为了转发端口。

神州数码 DCRS-7500 交换机提供了标准 STP（IEEE802.1d）和扩展 STP。扩展 STP 包括：

- 快速生成树协议（IEEE802.1w）
- 快速端口生成（Fast Port Span）
- 快速上行链生成（Fast Uplink Span）
- PerVLAN STP(PVST)

## 4.2 配置标准 STP 参数

神州数码 DCRS-7500 交换机支持标准 STP。在二层交换机上，STP 默认开启；在三层交换机上，STP 默认关闭。

默认状态下，每个基于端口的 VLAN 都运行各自的 STP。当用户添加了一个基于端口的 VLAN 时，这个 VLAN 会运行自己的 STP，这个 STP 的参数与 VLAN 1 的参数一致。用户可以配置开启或关闭每个 VLAN 的 STP，还可以开启或关闭每个端口的 STP。

### 4.2.1 STP 参数和默认状态

表 4.1 列出了默认 STP 网桥参数。参数全局有效。

表 4.1：默认 STP 网桥参数

| 参数 | 描述 | 默认状态和取值范围 |
|---|---|---|
| 转发延迟（Forward Delay） | 网络拓扑发生变化时，网桥重新转发前所等待的时间（listen 和 learn 之和) | 15 seconds<br>取值范围： 4 – 30 seconds |
| 网桥最大老化时间（Bridge Max Age） | The interval a bridge will wait for a hello packet from the root bridge before initiating a topology change. | 20 seconds<br>取值范围： 6 – 40 seconds |
| Hello Time | 根网桥发送 BPDU 包的时间间隔 | 2 seconds<br>取值范围： 1 – 10 seconds |
| 优先级（Priority） | 用来定义根网桥的参数。最小值的网桥具有最高的优先级，成为根网桥。 | 32768 seconds<br>取值范围： 0 – 65535 seconds |

**注意：**几个定时器之间是有约束的，条件如下：

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

表 4.2 列出了默认 STP 端口参数。参数在端口有效，需要逐个端口配置。

表 4.2：默认 STP 端口参数

| 参数 | 描述 | 默认状态和取值范围 |
|---|---|---|
| 优先级（Priority） | 生成树中一个端口相对与其他端口转发数据的优先选择。<br>取值越高，优先级越低。取值为 0 时，优先级最高。 | 128<br>取值范围： 0 – 255 |
| 路径代价（Path Cost） | 从端口到根网桥的总代价。当从端口到根网桥存在多条路径时，生成树使用代价最小的路径，阻断其他路径。不同类型的端口有不同的默认代价值。 | 10 Mbps – 100<br>100 Mbps – 19<br>Gigabit – 4<br>取值范围： 0 – 65535 |

### 4.2.2 开启的关闭 STP

用户可以在下列级别上启用和关闭 STP：

- 全局（Globally）：对交换机上所有端口生效。
- 基于端口的 VLAN（Port-based VLAN）：只在指定的基于端口的 VLAN 内生效。当用户设定基于端口的 VLAN 时，其配置会覆盖全局配置。当全局 STP 关闭时，用户仍然

可以开启基于端口的 VLAN。或者当全局 STP 开启时，用户仍然可以关闭基于端口的 VLAN。

- 基于端口：只对指定端口生效：当用户改变链路聚合组中的主端口的 STP 状态时，这些改变同样会对链路聚合组中其他端口生效。

#### 4.2.2.1 全局开启的关闭 STP

命令： [no] spanning-tree
功能： 全局开启的关闭 STP
命令模式： 全局配置模式
举例：

```
DCRS-7500(config)# spanning-tree
```

上述命令使交换机上每个 VLAN（包括默认的 VLAN）都有单独的 STP。

#### 4.2.2.2 开启的关闭基于端口的 VLAN 的 STP

命令： [no] spanning-tree
功能： 开启的关闭基于端口的 VLAN 的 STP
命令模式： VLAN 配置模式
举例：

```
DCRS-7500(config)# vlan 10
DCRS-7500(config-vlan-10)# spanning-tree
```

上述命令在 VLAN10 上开启 STP。

#### 4.2.2.3 开启和关闭基于端口的 STP

命令： [no] spanning-tree
功能： 开启的关闭基于端口的 STP
命令模式： 端口配置模式
举例：

```
DCRS-7500(config)# interface 1/1
DCRS-7500(config-if-1/1)# spanning-tree
```

上述命令在端口 1/1 上开启 STP。

### 4.2.3 改变 STP 网桥和端口参数

表 4.1 和表 4.2 列出了 STP 网桥和端口的默认参数，用户可以修改这些参数。

#### 4.2.3.1　改变 STP 网桥参数

命令：　[no] spanning-tree [forward-delay <value>] | [hello-time <value>] | [maximum-age <value>] | [priority <value>]

功能：　改变 STP 网桥参数

命令模式：　全局配置模式或 VLAN 配置模式

参数：　forward-delay <value>表示转发延迟，取值范围使是：4-30，默认值是 15；

hello-time <value>表示根网桥发送 BPDU 包的时间间隔，取值范围使是：1-10，默认值是 2；

maximum-age <value>表示网桥最大老化时间，取值范围使是：6-40，默认值是 20；

priority <value>表示优先级，取值越大优先级越小。取值范围是 0-65535，默认值是 32768。

举例一：

```
DCRS-7500(config)# spanning-tree priority 0
```

上述命令把交换机的网桥优先级设定为 0，使其成为根网桥。

举例二：

```
DCRS-7500(config)# vlan 20
DCRS-7500(config-vlan-20)# spanning-tree priority 0
```

上述命令把 VLAN 20 的网桥优先级设定为 0。

#### 4.2.3.2　改变 STP 端口参数

命令：　spanning-tree ethernet <portnum> path-cost <value> | priority <value>

功能：　改变 STP 端口参数

命令模式：　VLAN 配置模式

参数：　ethernet <portnum>指定端口号码；

path-cost <value>指定端口到根网桥的代价，STP 选取代价最小的。它的取值范围是 0-65535，默认值取决与端口类型：

10 Mbps – 100

100 Mbps – 19

Gigabit – 4

priority <value>表示生成树中端口相对与其他端口转发数据的优先选择。取值范围是 0-255，默认值是 128。取值越高，优先级越低。取值为 0 时，优先级最高。

举例：

```
DCRS-7500(config)# vlan 10
DCRS-7500(config-vlan-10)# spanning-tree ethernet 1/5 path-cost 15 priority 64
```

上述命令把 VLAN 10 中端口 1/5 的路径代价设定为 15，优先级设定为 64。

## 4.2.4 显示 STP 信息

### 4.2.4.1 显示交换机的 STP 信息

命令： show span [vlan <vlan-id>] | [pvst-mode] | [<num>]
功能： 显示交换机的 STP 信息
命令模式： 全局配置模式
举例：

```
DCRS-7500(config)# show span

Global STP Parameters:

VLAN Root         Root     Root     Prio     Max He- Ho- Fwd Last     Chg Bridge
ID   ID           Cost     Port     rity     Age llo ld  dly Chang    cnt Address
                                    Hex      sec sec sec sec sec
1    800000e052a9bb40 0 Root        8000     20  2   2   15  0        6 00e052a9bb40

Port STP Parameters:

VLAN     Port  Prio  Path  State    Fwd   Design   Design       Design
ID       Num   rity  Cost           Trans  Cost    Root         Bridge
Hex
1        3/1   80    19    ENABLED  2     0    800000e052a9bb40 800000e052a9bb40
1        3/2   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/3   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/4   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/5   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/6   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/7   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/8   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/9   80    0     DISABLED 0     0    0000000000000000 0000000000000000
1        3/10  80    0     DISABLED 0     0    0000000000000000 0000000000000000
```

### 4.2.4.2 显示 CPU 利用统计数据

命令： show process cpu [<num>]
功能： 显示 CPU 利用统计数据
命令模式： 特权配置模式
参数： The <num> parameter specifies the number of seconds and can be from 1 – 900. If you use this parameter, the command lists the usage statistics only for the specified number of seconds. If you do not use this parameter, the command lists the usage statistics for the previous one-second, one-minute, five-minute, and fifteen-minute intervals.

举例一：

```
DCRS-7500# show process cpu
Process Name     5Sec(%)     1Min(%)     5Min(%)     15Min(%)    Runtime(ms)
ARP              0.01        0.00        0.00        0.00        0
ICMP             0.01        0.00        0.00        0.00        1
IP               0.00        0.00        0.00        0.00        0
OSPF             0.00        0.00        0.00        0.00        0
RIP              0.00        0.00        0.00        0.00        0
STP              0.00        0.00        0.00        0.00        0
VRRP             0.00        0.00        0.00        0.00        0
```

举例二：

```
DCRS-7500# show process cpu 2
Statistics for last 1 sec and 80 ms
Process Name     Sec(%)  Time(ms)
ARP              0.00    0
ICMP             0.01    1
IP               0.00    0
OSPF             0.00    0
RIP              0.00    0
STP              0.01    0
VRRP             0.00    0
```

#### 4.2.4.3　显示基于端口 VLAN 的 STP 状态

## 4.3 配置扩展 STP

### 4.3.1 快速端口生成（Fast Port Span）

交换机上运行 STP 时，当网络拓扑变化，重新进行生成树计算时，流量转发会出现延迟。STP 转发延迟表示网桥在转发数据包前等待的时间。转发延迟控制 STP 重新收敛（convergence）的侦听（listening）和学习（learning）阶段。

用户可以设置转发延迟的值：从 4 秒到 30 秒，默认是 15 秒。所以在默认状态下，收敛需要 30（15 秒侦听和 15 秒学习）。

在一些情况下，这种缓慢的收敛时间是不必要的。快速端口生成功能允许特定端口在 4 秒中转换到转发状态。快速端口生成一般用于连接客户终端（end station）的端口，因为这些端口不会造成潜在的二层环路。

快速端口生成还有助于交换机整体性能的提高。快速端口生成减少了网络拓扑结构变化通告。当交换机端口连接的客户终端启动或宕机时，交换机不会产生网络变化通告，因为这种变化不影响网络拓扑结构。

快速端口生成是系统级的特性，默认状态下是开启的。

快速端口生成不能用于下列环境：

- 端口是 802.1q 标签端口
- 端口属于一个链路聚合组（trunk group）
- 端口有超过 1 个活动的 MAC 地址

命令： [no] fast port-span

功能： 开启快速端口生成

命令模式： 全局配置模式

举例一：

```
DCRS-7500(config)# no fast port-span
DCRS-7500(config)# write memory
```

上述命令关闭交换机的快速端口生成，这种配置在交换机不直连客户终端，而只连接其他交换机时十分有用。

举例二：

```
DCRS-7500(config)# fast port-span
DCRS-7500(config)# write memory
```

上述命令在交换机上开启快速端口生成。

# 第5章 配置 Virtual LANs（VLAN）

本章主要阐述神州数码 DCRS-7500 二、三层交换机上如何配置 VLAN.

## 5.1 VLAN 的种类

神州数码 DCRS-7500 交换机可以配置如下种类的 VLAN：

- 二层基于端口的 VLAN（Layer 2 port-based VLAN）：一组物理端口共享二层广播域
- IP 子网 VLAN（IP sub-net VLAN）：一组基于端口 VLAN 的子集，由 IP 子网构成的 VLAN

当交换机上 VLAN 的端口收到 1 个数据包时，交换机按照下列顺序转发数据包：

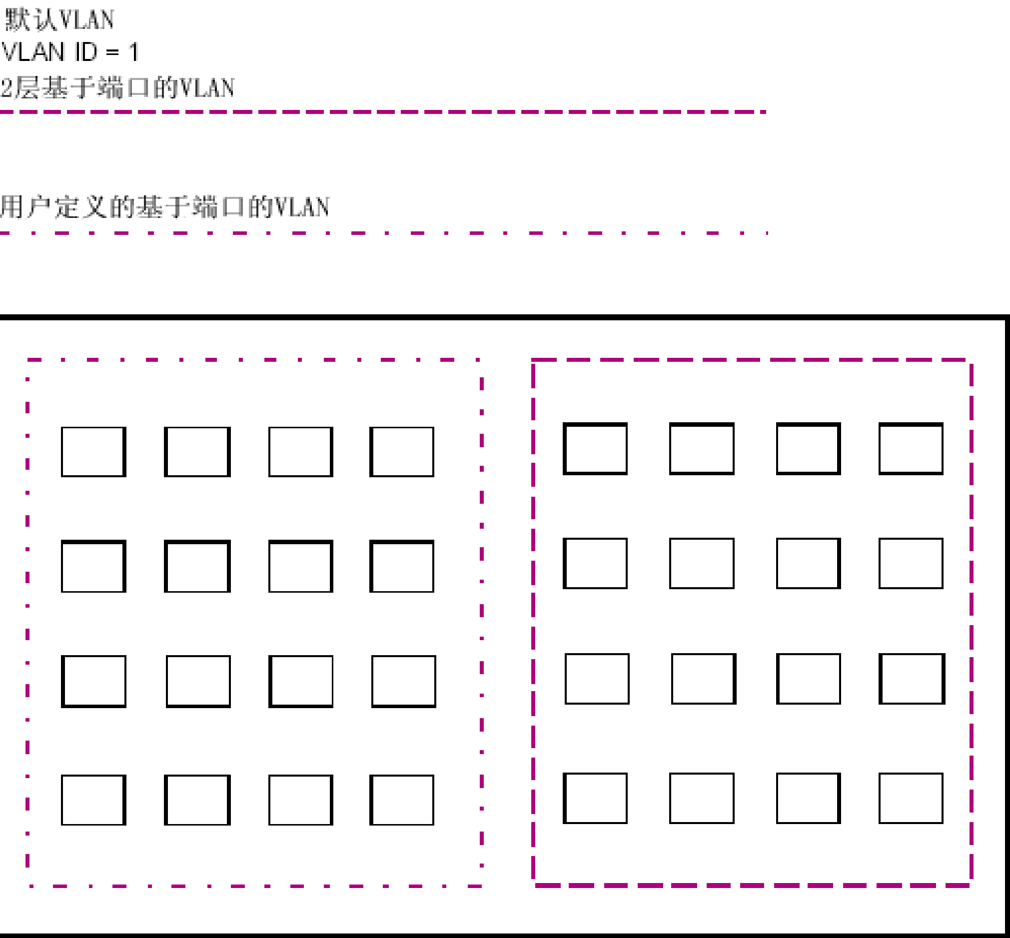
- 如果端口属于 IP 子网 VLAN，交换机把数据包转发到这个 IP 子网 VLAN 内的所有端口；
- 如果数据包不符合上面的转发条件，但端口属于二层基于端口的 VLAN，交换机把数据包转发到这个二层基于端口的 VLAN 内的所有端口。

### 5.1.1 二层基于端口的 VLAN

用户可以在交换机上配置基于端口的 VLAN。基于端口的 VLAN 是交换机上一些端口的集合，这些端口组成 1 个二层广播域。

默认状态下，交换机上所有的端口都属于默认的 VLAN，这个 VLAN 构成单一的 1 个二层广播域。用户可以配置多个基于端口的 VLAN，当用户添加 1 个基于端口的 VLAN 时，交换机自动把新添加 VLAN 的端口从默认 VLAN 中清除。

图 5.1：二层基于端口的 VLAN



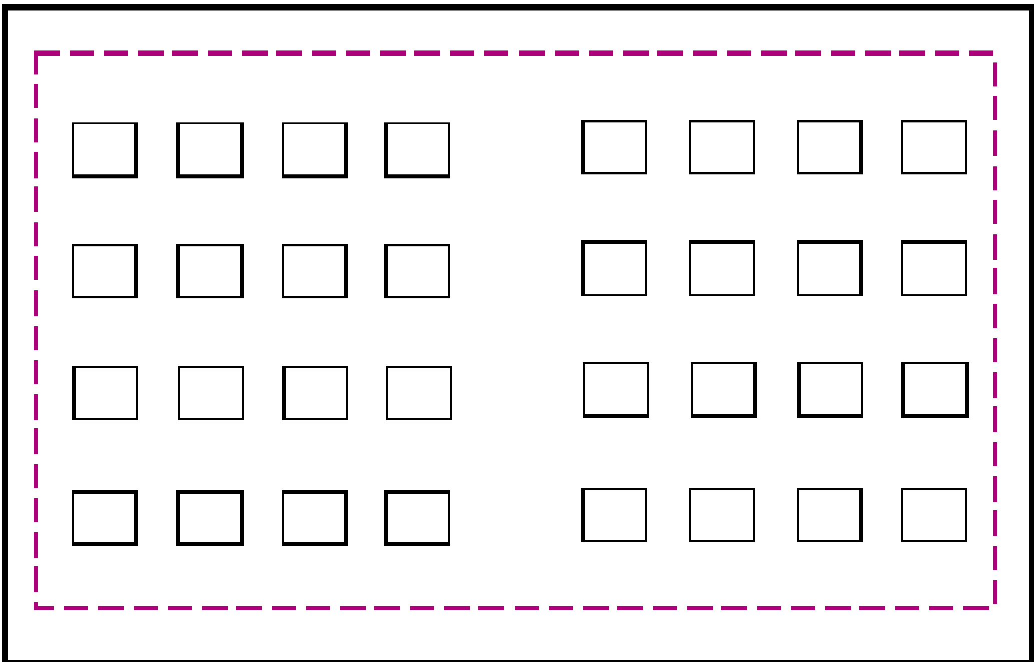

1 个端口只能属于 1 个基于端口的 VLAN，除非这个端口是 802.1q 端口。***802.1q Tagging***（802.1q 标签）给所有发送到端口数据包添加 1 个 4 位（four-byte）的标签（tag），标签中包含 VLAN ID。标签使交换机能够判定收到的数据包属于哪个 VLAN。802.1q 标签只能应用于二层 VLAN，而不能应用于三层 VLAN。

因为每个基于端口的 VLAN 都是 1 个二层广播域，所以默认状态下每个 VLAN 运行单独的 STP。在基于端口 VLAN 内部，二层流量采用桥接，二层广播会发送到 VLAN 内所有端口。

### 5.1.2 默认 VLAN

默认状态下，交换机上所有的端口都属于 1 个基于端口的 VLAN，这个 VLAN 被成为默认 VLAN（DEFAULTVLAN），VLAN 号为 1。

图 5.2：默认二层基于端口的 VLAN




当用户在交换机上配置基于端口的 VLAN 时，交换机会自动把添加到这个 VLAN 中的端口从默认 VLAN 中清除，这样能保证每个端口只属于 1 个二层广播域。

一些网络配置需要 1 个端口属于 2 个或多个二层广播域，这时需要给端口加标签以确认数据包属于哪个 VLAN。

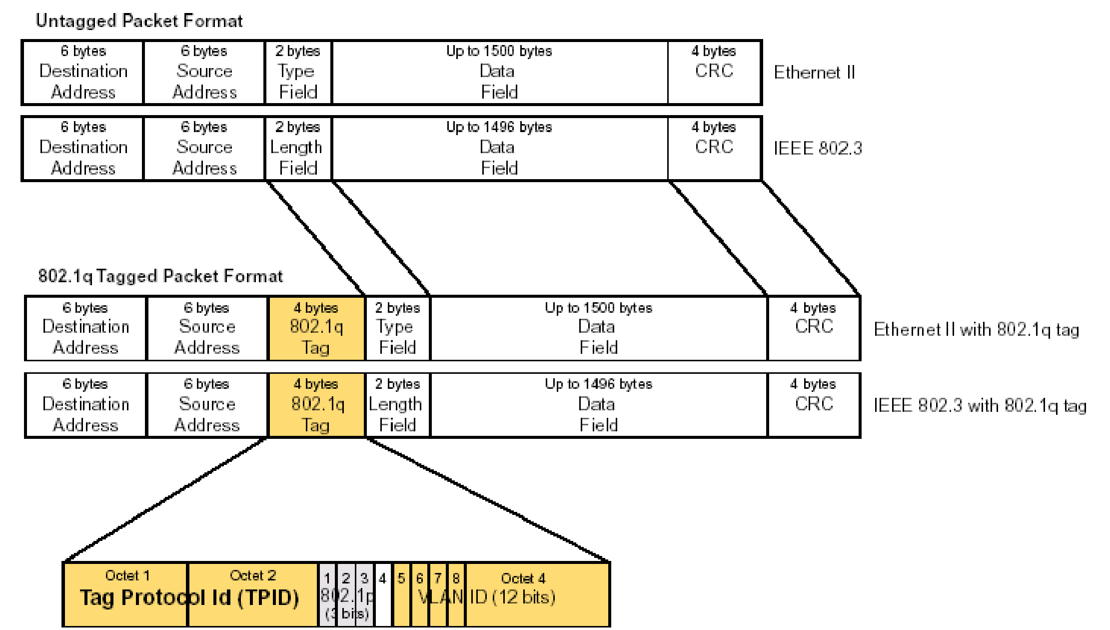
## 5.1.3 802.1q Tagging（802.1q 标签）

802.1q 标签是一项 IEEE 的标准，它允许网络设备在二层数据包加入鉴别 VLAN 成员的信息。神州数码 DCRS-7500 交换机在数据包中加入一个 4 字节的标签，这个标签包括标签值（tag value）和 VLAN ID。标签值确定后续数据为标签，VLAN ID 决定了数据包属于哪个 VLAN。

- 默认的标签值是 8100（十六进制）：当与其他厂家交换机互联时，这个值可以全局改变。
- VLAN ID 决定数据包被转发到的 VLAN

图 5.3 显示了数据包包括和不包括 802.1q 标签的格式。不同厂商的标签格式不同，因此互联不同厂商设备时要确认格式是否一致。

图 5.3：802.1q 标签格式




当用户配置 1 个跨越多个交换机的 VLAN 时，如果与另一台交换机相连的端口属于多个 VLAN 时，端口需要加标签；如果与另一台交换机相连的端口只属于 1 个 VLAN 时，端口不需要加标签。

如果在多台交换机上使用标签，必须使用相同的标签格式。

## 5.2 配置基于端口的 VLAN

本节阐述如何进行以下基于端口 VLAN 的配置：

- 创建 VLAN
- 删除 VLAN
- 修改 VLAN
- 改变 VLAN 的优先级
- 开启和关闭 VLAN 的 STP

### 5.2.1 创建 VLAN

命令： vlan <vlan-id> by port

功能： 添加基于端口的 VLAN

命令模式： 全局配置模式
参数： <vlan-id>指定创建 VLAN 的 ID

命令： untagged ethernet <portnum> [to <portnum> | ethernet <portnum>]
功能： 添加不带标签的端口到 VLAN
命令模式： VLAN 配置模式
参数： <portnum>指定端口号；to <portnum> | ethernet <portnum>指定端口范围
举例：

```
DCRS-7500(config)# vlan 222 by port
DCRS-7500(config-vlan-222)# untag e 1 to 8
DCRS-7500(config-vlan-222)# vlan 333 by port
DCRS-7500(config-vlan-333)# untag e 9 to 16
```

上述命令创建基于端口的 VLAN222，包括不带标签的端口 1 到 8；创建基于端口的 VLAN333，包括不带标签的端口 9 到 16。

### 5.2.2 删除 VLAN

命令： no vlan <vlan-id> by port
功能： 删除基于端口的 VLAN
命令模式： 全局配置模式
参数： <vlan-id>指定删除 VLAN 的 ID
举例：

```
DCRS-7500(config)# no vlan 5
DCRS-7500(config)# end
DCRS-7500# write memory
```

上述命令删除 VLAN5。

### 5.2.3 修改 VLAN

命令： no untagged ethernet <portnum> [to <portnum> | ethernet <portnum>]
功能： 从 VLAN 中删除不带标签的端口
命令模式： VLAN 配置模式
参数： <portnum>指定端口号；to <portnum> | ethernet <portnum>指定端口范围
举例：

```
DCRS-7500(config)# vlan 4
DCRS-7500(config-vlan-4)# no untag ethernet 11
DCRS-7500(config-vlan-4)# end
```

上述命令从 VLAN4 中删除端口 11。

### 5.2.4 改变 VLAN 的优先级

命令：　　　priority normal | high
功能：　　　改变 VLAN 的优先级
命令模式：　VLAN 配置模式
参数：　　　normal | high 分别表示正常优先级和高优先级
举例：

```
DCRS-7500(config)# vlan 2
DCRS-7500(config-vlan-2)# priority high
DCRS-7500(config-vlan-2)# end
```

上述命令给 VLAN2 分配较高优先级。

### 5.2.5 开启和关闭 VLAN 的 STP

命令：　　　[no] spanning-tree
功能：　　　开启和关闭 STP
命令模式：　VLAN 配置模式
举例：

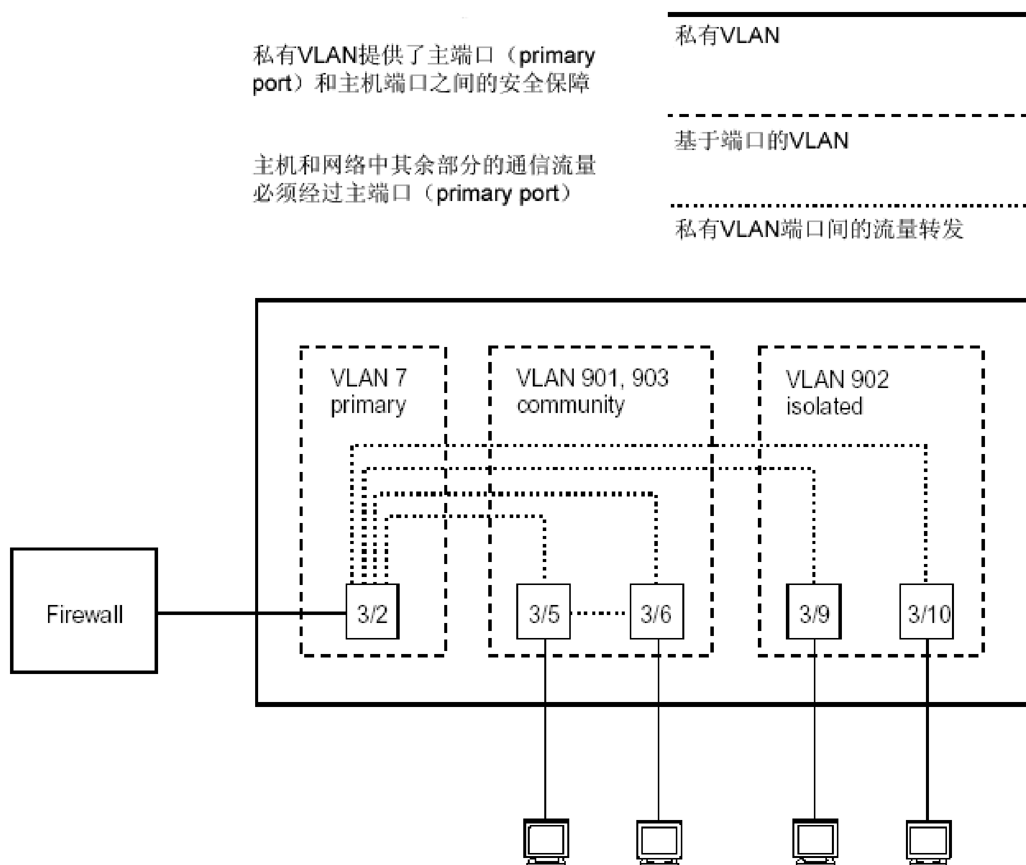
```
DCRS-7500(config)# vlan 3
DCRS-7500(config-vlan-3)# spanning-tree
DCRS-7500(config-vlan-3)# end
```

上述命令开启 VLAN3 的 STP。

## 5.3 私有 VLAN（Private VLAN）

私有 VLAN 既具有二层基于端口 VLAN 的属性又提供了对于进出 VLAN 流量的额外限制，图 5.4 显示了一个私有 VLAN 的例子。

图 5.4：私有 VLAN 举例




上述例子中，私有 VLAN 通过防火墙（firewall）提供了主机和网络其余部分的安全性。例子中的 5 个端口都是私有 VLAN 的成员。端口 3/2 连接到防火墙，端口 3/5, 3/6, 3/9 和 3/10 连接到主机上，这些主机依靠防火墙提供和网络其余部分的安全性。端口 3/5 和 3/6 在公共（community）私有 VLAN，它们可以相互访问，还可以访问防火墙。端口 3/9 和 3/10 在隔离（isolated）私有 VLAN，它们不能相互访问，只能访问防火墙。

用户可以配置下列私有 VLAN:

- 主（Primary）私有 VLAN：主私有 VLAN 的端口是“混杂”（“promiscuous”）端口。这些端口可以和公共私有 VLAN 和隔离私有 VLAN 中的所有端口通信，只要这些公共私有 VLAN 和隔离私有 VLAN 中的端口映射到主私有 VLAN 端口。
- 隔离（isolated）私有 VLAN：隔离私有 VLAN 的端口只能同主私有 VLAN 的端口通信，它们相互之间不能通信。
- 公共（community）私有 VLAN：公共私有 VLAN 中的端口能相互通信，并可以和主私有 VLAN 的端口通信。

每个私有 VLAN 必须有 1 个主私有 VLAN。主私有 VLAN 位于安全端口和其余网络之间。

表 5.1：私有 VLAN 和基于端口的 VLAN 比较

| 转发行为 | 私有 VLAN | 基于端口的 VLAN |
| --- | --- | --- |
| VLAN 中的所有端口组成 1 个广播域 | 否 | 是 |
| 广播和未知单播默认转发到 VLAN 中所有端口 | 否 | 是 |
| VLAN 中的端口能够相互发送和接受单播流量 | 否（隔离私有 VLAN）<br>是（主私有 VLAN 和公共私有 VLAN） | 是 |

## 5.3.1 配置私有 VLAN

配置私有 VLAN 时，要把每种私有 VLAN 分别配置到 1 个基于端口的 VLAN 中。配置步骤是：

- 使用标准 VLAN 配置命令创建 VLAN 并添加端口
- 指定私有 VLAN 类型（主私有 VLAN、隔离私有 VLAN 或公共私有 VLAN）
- 对于主私有 VLAN，要把其他私有 VLAN 映射到主私有 VLAN 的端口上

配置规则：

- 用户可以在 10/100/1000 兆以太网端口配置私有 VLAN；
- 私有 VLAN 的端口不能是端口聚合组的成员；
- 1 个端口不能既属于私有 VLAN 又属于标准基于端口的 VLAN；
- 每个基于端口的 VLAN 中只能配置 1 个私有 VLAN；
- 每个私有 VLAN 只能有 1 个主私有 VLAN；
- 每个私有 VLAN 可以有多个隔离私有 VLAN 和公共私有 VLAN；
- 3 种私有 VLAN 中的端口可以是加标签（tagged）的或不加标签的（untagged）；
- 主私有 VLAN 中可以有多个端口，但只能有一个端口被激活，其余的作为冗余；
- 不能把默认 VLAN 配置成私有 VLAN。

### 5.3.1.1　配置隔离私有 VLAN 和公共私有 VLAN

命令：　　[no] pvlan type community | isolated | primary

功能：　　指定私有 VLAN 类型

命令模式：VLAN 配置模式

参数：　　community | isolated | primary 指定私有 VLAN 的类型

举例：

```
DCRS-7500(config)# vlan 901
DCRS-7500(config-vlan-901)# tagged ethernet 3/5 to 3/6
DCRS-7500(config-vlan-901)# pvlan type community
```

上述命令创建公共私有 VLAN901，并把端口 3/5 和 3/6 加入到这个 VLAN。

#### 5.3.1.2 配置主私有 VLAN

命令： [no] pvlan mapping <vlan-id> ethernet <portnum>
功能： 映射隔离私有 VLAN 和公共私有 VLAN 到主私有 VLAN
命令模式： VLAN 配置模式
参数： <vlan-id>指定另外 1 个已经配置好的私有 VLAN，把该 VLAN 映射到这个主私有 VLAN 上；ethernet <portnum>表示把上述已经配置好的私有 VLAN 映射到哪个主私有 VLAN 的端口
举例：

```
DCRS-7500(config)# vlan 7
DCRS-7500(config-vlan-7)# untagged ethernet 3/2
DCRS-7500(config-vlan-7)# pvlan type primary
DCRS-7500(config-vlan-7)# pvlan mapping 901 ethernet 3/2
```

上述命令创建主私有 VLAN7，把端口 3/2 加入到该 VLAN，并把私有 VLAN901 映射到主私有 VLAN 端口

#### 5.3.1.3 开启向私有 VLAN 内转发广播和未知单播（Unknown Unicast）

为了加强私有 VLAN 的安全性，私有 VLAN 不会转发广播和未知单播流量到隔离私有 VLAN 和公共私有 VLAN。例如，图？？中的端口 3/2 收到防火墙发来的广播流量，不会转发到其他私有 VLAN 端口（端口 3/5, 3/6, 3/9 和 3/10）。

但是，主私有 VLAN 收到从隔离私有 VLAN 和公共私有 VLAN 发来的广播和未知单播，会被转发到防火墙上。例如，端口 3/9 上的主机发送的未知单播会被端口 3/2 转发到防火墙上。

用户何以通过配置来开启向私有 VLAN 内转发广播或未知单播。

命令： [no] pvlan-preference broadcast | unknown-unicast flood
功能： 开启向私有 VLAN 内转发广播或未知单播
命令模式： 全局配置模式
参数： broadcast | unknown-unicast flood 指定了允许向私有 VLAN 内转发的流量类型：广播或未知单播
举例一：

```
DCRS-7500(config)# pvlan-preference broadcast flood
DCRS-7500(config)# pvlan-preference unknown-unicast flood
```

上述命令开启向私有 VLAN 内转发广播和未知单播。

举例二：

```
DCRS-7500(config)# no pvlan-preference broadcast flood
```

上述命令关闭向私有 VLAN 内转发广播。

#### 5.3.1.4　配置举例

配置图？？中的私有 VLAN，需要进行以下配置：

```
DCRS-7500(config)# vlan 901
DCRS-7500(config-vlan-901)# tagged ethernet 3/5 to 3/6
DCRS-7500(config-vlan-901)# pvlan type community
DCRS-7500(config-vlan-901)# exit
DCRS-7500(config)# vlan 902
DCRS-7500(config-vlan-902)# tagged ethernet 3/9 to 3/10
DCRS-7500(config-vlan-902)# pvlan type isolated
DCRS-7500(config-vlan-902)# exit
DCRS-7500(config)# vlan 903
DCRS-7500(config-vlan-903)# tagged ethernet 3/5 to 3/6
DCRS-7500(config-vlan-903)# pvlan type community
DCRS-7500(config-vlan-903)# exit
DCRS-7500(config)# vlan 7
DCRS-7500(config-vlan-7)# untagged ethernet 3/2
DCRS-7500(config-vlan-7)# pvlan type primary
DCRS-7500(config-vlan-7)# pvlan mapping 901 ethernet 3/2
DCRS-7500(config-vlan-7)# pvlan mapping 902 ethernet 3/2
DCRS-7500(config-vlan-7)# pvlan mapping 903 ethernet 3/2
```

## 5.4 显示端口信息

配置完 VLAN 后，用户可以使用下面命令查看配置。

命令：　　show vlans [<vlan-id> | ethernet <portnum>]
功能：　　显示 VLAN 信息
命令模式：特权配置模式
参数：　　<vlan-id>指定显示特定 VLAN 的 VLAN 信息；
　　　　　ethernet <portnum>指定显示特定端口的 VLAN 信息

举例一：

```
DCRS-7500(config)# show vlans

Total PORT-VLAN entries: 2
Maximum PORT-VLAN entries: 8
legend: [S=Slot]

PORT-VLAN 1, Name DEFAULT-VLAN, Priority level0, Spanning tree Off
  Untagged Ports: (S2) 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
  Untagged Ports: (S2) 17 18 19 20 21 22 23 24
```

```
  Untagged Ports: (S4) 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
  Untagged Ports: (S4) 17 18 19 20 21 22 23 24
    Tagged Ports: None

PORT-VLAN 10, Name IP_VLAN, Priority level0, Spanning tree Off
  Untagged Ports: (S1) 1 2 3 4 5 6
    Tagged Ports: None

IP-subnet VLAN 1.1.1.0 255.255.255.0, Dynamic port enabled
        Name: Mktg-LAN
Static ports: None
Exclude ports: None
Dynamic ports: (S1) 1 2 3 4 5 6
PORT-VLAN 20, Name IPX_VLAN, Priority level0, Spanning tree Off
Untagged Ports: (S2) 1 2 3 4 5 6
  Tagged Ports: None

IPX-network VLAN 0000ABCD, frame type ethernet_ii, Dynamic port enabled
          Name: Eng-LAN
  Static ports: None
Exclude ports: None
Dynamic ports: (S2) 1 2 3 4 5 6
```

上述命令显示了交换机上全部的 VLAN 信息。

举例二：

```
DCRS-7500(config)# show vlans e 7/1

Total PORT-VLAN entries: 3
Maximum PORT-VLAN entries: 8

legend: [S=Slot]

PORT-VLAN 100, Name [None], Priority level0, Spanning tree Off
Untagged Ports: (S7) 1 2 3 4
  Tagged Ports: None

  IP-subnet VLAN 207.95.11.0 255.255.255.0, Dynamic port disabled
  Static ports: (S7) 1 2
  Exclude ports: None
  Dynamic ports: None
```

上述命令显示端口 7/1 上的 VLAN 信息。

# 第6章 配置 GARP VLAN Registration Protocol (GVRP)

GARP VLAN Registration Protocol (GVRP)协议提供了动态注册和分配 VLAN 的机制。神州数码 DCRS-7500 交换机提供下列 GVRP 功能：

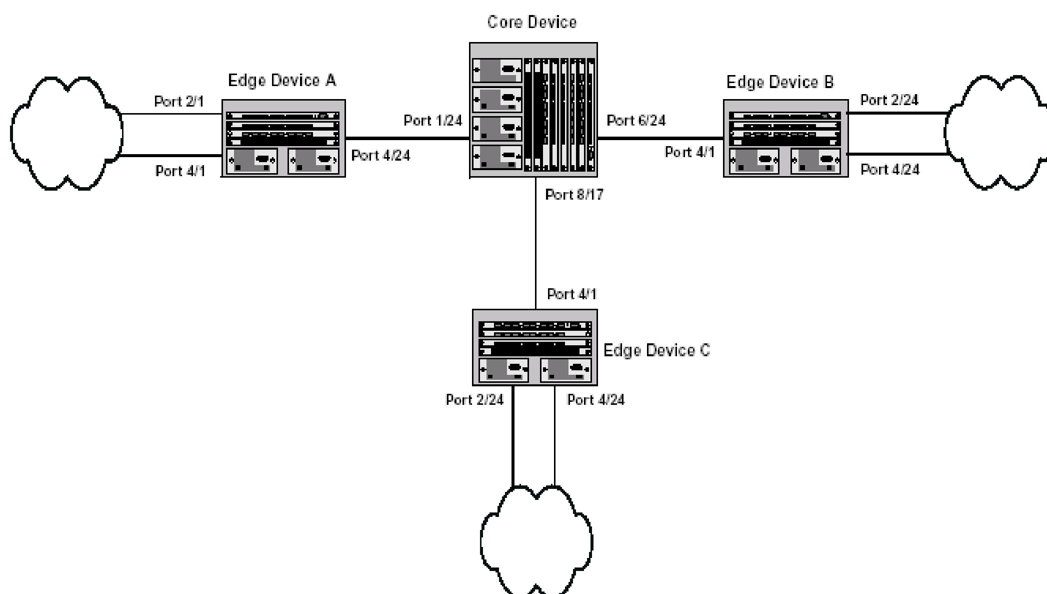
- 学习其他交换机的 VLAN 信息并在学习 VLAN 信息的端口上配置这些 VLAN 信息。交换机侦听其他交换机发出的 GVRP Protocol Data Units (PDUs)包，按照 GVRP PDU 包中的信息进行 VLAN 配置。
- 向其他交换机通告本机配置的 VLAN 信息。配置了 GARP 的交换机通过发送 GVRP PDU 包来向其他交换机传送静态配置的 VLAN 信息和通过 GVRP 学习到的 VLAN 信息。

GVRP 使交换机能够在与其他交换机运行 GVRP 的端口动态建立 802.1Q VLAN。GVRP 能够使跨网络 VLAN ID 自动保持一致，从而减少了 VLAN 出错的可能性。配置了 GVRP 的交换机可以自动向其他 GVRP 交换机通告 VLAN 信息，无需手工在每一个交换机上作配置。并且，当一台交换机的 VLAN 配置发生变化时，GVRP 能够自动改变其他交换机的相应配置。

## 6.1 GVRP 配置组合

我们通过 1 个示例来了解一下配置 GVRP 的 4 种组合。

图 6.1：GVRP 示例




在这个示例中，一台中心设备连接三台边缘设备。每台边缘设备又连接到其它边缘设备

或主机工作站。在该网络中启用 GVRP 的作用取决于该网络中被激活的设备的属性，以及学习(learning)和通告(advertising)是否都被启用。在这种类型的网络中，一共有四中组合：

- 动态核心(Dynamic core)和固定边缘(Fixed edge)
- 动态核心(Dynamic core)和动态边缘(Dynamic edge)
- 固定核心(Fixed core)和动态边缘(Dynamic edge)
- 固定核心(Fixed core)和固定边缘(Fixed edge)

### 6.1.1 动态核心(Dynamic core)和固定边缘(Fixed edge)

在这种配置模式下，所有位于核心设备上的端口都被启用以用于学习和通告 VLAN 的信息。边缘设备都被配置成通过连接到核心设备的端口向核心设备通告 VLAN 的信息。GVRP 的学习功能在边缘设备上是关闭的。

表 6.1：动态核心和固定边缘

| 核心设备 | 边缘设备 A | 边缘设备 B | 边缘设备 C |
|---|---|---|---|
| GVRP 在所有端口上都被启用，学习和通告都被启用<br>**注意：**<br>既然所有边缘设备的学习功能是禁止的，核心设备上的通告功能配置就没有作用。 | GVRP 在端口 4/24 上被启用；学习功能被禁用。<br>VLAN20<br>Port2/1(untagged)<br>Port4/24(tagged)<br>VLAN40<br>Port4/1(untagged)<br>Port4/24(tagged) | GVRP 在端口 4/1 上被启用；学习功能被禁用。<br>VLAN20<br>Port2/24(untagged)<br>Port4/1(tagged)<br>VLAN30<br>Port4/24(untagged)<br>Port4/1(tagged) | GVRP 在端口 4/1 上被启用；学习功能被禁用。<br>VLAN30<br>Port2/24(untagged)<br>Port4/1(tagged)<br>VLAN40<br>Port4/24(untagged)<br>Port4/1(tagged) |

在这种配置方式(动态核心和固定边缘)下，边缘设备被静态地（手工地）配置 VLAN 信息。核心设备动态地配置自己为每一个边缘设备的 VLAN 成员。在核心设备上操作的结果是下面的 VLAN 信息配置到该设备上：

VLAN 20
1/24(tagged)
6/24(tagged)
VLAN 30
6/24(tagged)
8/18(tagged)
VLAN 40
1/24(tagged)
8/17(tagged)

现在 VLAN 20 的数据流可以通过核心设备流经边缘设备 A 和设备 B。同样，VLAN 30 的数据流可以在设备 B 和设备 C 之间传输，VLAN 40 的数据流可以在设备 A 和设备 C 之间传输。如果一台边缘设备被移动至核心设备的一个不同端口或者一台边缘设备的 VLAN 配置发生变化，核心设备会自动重新配置自己以适应这种变化。

请注意在动态创建的 VLAN 的每个端口被标记（tagged）。所有的被 GVRP 配置的 GVRP VLAN 端口被标记以确保该端口可被另外的 VLAN 配置。

**注意**：本例中假设核心设备没有被静态配置。然而，可以先配置一台设备运行 GVRP。GVRP 可以动态地加入其它端口至静态配置的 VLAN，然而，却不能从 VLAN 上删除静态配置的端口。

### 6.1.2 动态核心(Dynamic core)和动态边缘(Dynamic edge)

GVRP 在核心设备和边缘设备上启用。如果边缘云图中的设备运行的是 GVRP，并且把它们的 VLAN 信息通告给边缘设备，这种配置是比较有用的。边缘设备学习 VLAN 信息并且把它们通告该核心设备。尽管可以在设备上配置 VLAN 信息，但在这种配置下，不必要在边缘或核心设备上静态配置 VLAN 信息。这些设备可以从边缘云图中学到 VLAN 信息。

### 6.1.3 固定核心(Fixed core)和动态边缘(Dynamic edge)

GVRP 的学习功能在边缘设备上被启用。在核心设备上的 VLAN 信息被静态配置，并且核心设备启用通告功能以通告自己的 VLAN 信息，但不用于学习 VLAN 信息。边缘设备学习从核心设备学习 VLAN 信息。

### 6.1.4 固定核心(Fixed core)和固定边缘(Fixed edge)

VLAN 信息被静态地配置在核心和边缘设备上。在每一个边缘设备上，VLAN 通告(advertising)被启用，但学习(learning)功能被禁止。GVRP 没有在核心设备上启用。这种配置使得边缘云图中的去学习边缘设备的配置。

## 6.2 配置 GVRP

### 6.2.1 配置 GVRP 需要考虑的事项

配置 GVRP 时，下面几点是必须考虑的：

- 如果禁用 GVRP（no gvrp-enable）,保存（write memory）重启设备后，所有的 GVRP 配置信息将会丢掉。如果禁用 GVRP 后，没有先保存，重启设备后，GVRP 仍然是启用的。
- 一台设备支持的最大 VLAN 数量与该设备 GVRP 功能是否启用无关。
  - 可以使用命令：“show default values” 来显示在设备上支持的最大 VLAN 数量。在“VLAN”那一行中，确认缺省 VLAN 为 VLAN1,GVRP base VLAN(4093),Singel STP VLAN(4094).这些 VLAN 作为“Registration Forbidden”状态保存在 GVRP 数据库里，Registration Forbidden VLAN 不能通过 GVRP 学习和通告。
  - 为了增加交换机支持的 VLAN 数量，可以用命令：“system-max vlan <num>”来定义最大 VLAN 数量，执行此命令后，先要保存，再重新启动。设备可以支持的

VLAN 最大数量可以通过使用命令“show default values”来查看。

- 缺省 VLAN(VLAN1)不能通过神州数码 DCRS-7500 系列交换机执行 GVRP 功能来向外通告。 缺省 VLAN 包含所有没有被静态配置给 VLAN 的成员端口或启用了 GVRP 的 VLAN 端口。（**注意**：缺省 VLAN 的 ID 好为：1。仅仅在 GVRP 被启用之前，才可以修改缺省 VLAN 的 ID。反之，在启用了 GVRP 后，就不能再修改缺省 VLAN 的 ID 了。）
- Single STP 必须在设备上启用。神州数码的交换机启动 GVRP 需要启用 Single STP。如果没有在设备上静态地配置 VLAN，可以通过下面的命令来启用 Single STP:

```
DCRS-7500(config)#vlan 1
DCRS-7500(config-vlan-1)#exit
DCRS-7500(config)#span
DCRS-7500(config)#span single
```

  这几句命令启用缺省 VLAN(VLAN1)的配置：VLAN1 包含该设备的所有端口，并且启用了生成树协议和 Single STP。
- 所有通过 GVRP 动态学习到的 VLAN 被加入到单个的生成树(single spanning tree)。
- 所有为 GVRP 启用的端口变成 GVRP base VLAN(4093)标记成员（tagged member）。如果需要使用为另外的 VLAN 该 VLAN ID，可以改变 GVRP 的 VLAN ID。下面的“改变 GVRP Base VLAN ID”将详细介绍这部分内容。软件将把 GVRP base VLAN 加入到单个生成树（Single Spanning Tree）.
- 所有的通过 GVRP 加入的 VLAN 被标记（tagged）。
- GVRP 仅支持缺省 VLAN 成员中的标记端口(tagged)和非标记端口(untagged)。GVRP 不支持除了缺省 VLAN 以外的非标记端口。
- 在链路聚合组(trunk group)中配置 GVRP，只在该链路聚合组的主端口上启用该协议即可。在主端口上应用该协议可以自动被应用到该链路聚合组的其它端口上。
- 可以在一台已经静态配置了 VLAN 的设备上使用 GVRP。尽管 GVRP 可以加入端口到这个 VLAN 上，GVRP 不会从已经静态配置好的 VLAN 端口中移走任何端口。GVRP 通告这些静态配置的 VLAN。当保存这些配置文件时，被 GVRP 加入的端口不会在当前运行的配置文件(running-config)和备份的配置文件(startup-config)中显示出来。可以手工加入一个端口使其成为 VLAN 的永久成员。当手工加入一个端口后，这个端口将会在当前运行的配置文件中显示出来，当保存这些配置时，将被保存到备份的配置文件中去。
- 通过 GVRP 创建的 VLAN 不支持虚拟接口或基于协议的 VLAN。即使 GVRP 增加端口到这些 VLAN，虚拟接口和基于协议的 VLAN 仍将被静态配置的 VLAN 支持。
- 不可以在 GVRP 创建的 VLAN 上手工配置任何参数。比如，不能为 VLAN 改变生成树的参数。
- 使用 GVRP 交换 VLAN 信息时，所有设备上的 GVRP 记时器(Join、Leave and Leave all)必须被设置相同。
- 如果一个网络有很多的 VLAN，GVRP 的数据流可以使用大量的 CPU 资源。如果注意到很高的 CPU 消耗，可以设置记时器的值更长一些。尤其是把 Leave all 的值设置更长一些。这部分的设置可以参见下面：“更改 GVRP 的记时器”。

## 6.2.2 配置 GVRP

在神州数码 DCRS-7500 交换机上配置 GVRP 需要全局启用该功能，然后在特定端口上启用 GVRP。在特定端口上，可以选择关闭学习或通告功能。还可以改变 GVRP 的计时器（timers）和 GVRP base VLAN ID 号码。

### 6.2.2.1 改变 GVRP Base VLAN ID 号码

默认情况下，GVRP 使用 VLAN 4093 作为 GVRP 协议的基准 VLAN。所有启用了 GVRP 的端口都成为这个 VLAN 的标记（tagged）成员。如果要将 VLAN 4093 配置成静态 VLAN，可以改变 GVRP Base VLAN ID 号码。
**注意**：要改变 GVRP Base VLAN ID 号码，必须在启用 GVRP 前进行。

**命令**：　[no] gvrp-base-vlan-id <vlan-id>
**功能**：　改变 GVRP Base VLAN
**命令模式**：　全局配置模式
**参数**：　<vlan-id>为新的 GVRP Base VLAN ID 号码，取值范围是 2-4093 或 4095
**使用指南**：
**举例**：

```
DCRS-7500(config)# gvrp-base-vlan-id 1001
```

### 6.2.2.2 增加 Leaveall 计时器可配置的最大值

默认情况下，可以指定 Leaveall 计时器的最大值是 300000ms（毫秒），这个值可以被指定为最大 1000000 毫秒
**注意**：要改变 Leaveall 计时器的最大取值，必须在启用 GVRP 前进行。GVRP 启用后则无法改变。
**注意**：这条命令并不是改变 Leaveall 计时器的值，只是改变 Leaveall 计时器可以配置的最大值。

**命令**：　[no] gvrp-max-leaveall-timer <ms>
**功能**：　改变 Leaveall 计时器的最大取值
**命令模式**：　全局配置模式
**参数**：　<ms>为新的 Leaveall 计时器的最大取值，取值范围是 300000-1000000
**使用指南**：　<ms>值以 100 为增量
**举例**：

```
gvrp-max-leaveall-timer 1000000
```

#### 6.2.2.3 启用 GVRP

命令：　[no] gvrp-enable
功能：　启用 GVRP
命令模式：　全局配置模式
使用指南：　必须先使用该命令，然后在特定端口上启用 GVRP
举例：

```
gvrp-max-leaveall-timer 1000000
```

命令：　[no] enable all | ethenet <portnum>|[ethenet <portnum>|to <portnum>]
功能：　在端口上启用 GVRP
命令模式：　GVRP 配置模式
参数：　all表示在所有端口上启用GVRP；ethenet <portnum>|[ethenet <portnum>|to <portnum>]表示在特定以太端口和以太端口范围启用GVRP
举例一：

```
DCRS-7500(config-gvrp)# enable all
```

上述命令在所有端口上启用 GVRP。
举例二：

```
DCRS-7500(config-gvrp)# enable ethernet 1/24 ethernet 6/24 ethernet 8/17
```

上述命令在 port 1/24、6/24、8/17 启用 GVRP 功能。

#### 6.2.2.4 关闭 GVRP 的通告功能

命令：　[no] block-applicant all | ethernet <portnum> [ethernet <portnum> | to <portnum>]
功能：　关闭 GVRP 的通告功能
命令模式：　GVRP 配置模式
参数：　all表示关闭所有端口的GVRP通告功能；ethenet <portnum>|[ethenet <portnum>|to <portnum>]表示关闭特定以太端口和以太端口范围的GVRP通告功能
举例：

```
DCRS-7500(config-gvrp)# block-applicant ethernet 1/24 ethernet 6/24 ethernet
8/17
```

该命令关闭掉了端口 E 1/24、E 6/24、E 8/17 的 GVRP 通告功能。

#### 6.2.2.5 关闭 GVRP 的学习功能

命令：　[no] block-learning all | ethernet <portnum> [ethernet <portnum> | to <portnum>]
功能：　关闭 GVRP 的学习功能
命令模式：　GVRP 配置模式
参数：　all表示关闭所有端口的GVRP学习功能；ethenet <portnum>|[ethenet

<portnum>|to <portnum>]表示关闭特定以太端口和以太端口范围的GVRP学习功能

举例：

```
DCRS-7500(config)#blocking-learning ethernet 6/24
```

该命令把端口 E 6/24 的 GVRP 的学习功能关闭掉。

#### 6.2.2.6 改变 GVRP 计时器

GVRP 使用下列计时器：

- 加入计时器（Join）：交换机 GVRP 端口发送 VLAN 通告前等待的最大毫秒（ms）数。实际的加入时间间隔是随机产生的从 0 到指定加入计时器之间任意值。加入计时器的取值范围是从 200 到离开计时器的 1/3；默认值是 200 毫秒。
- 离开计时器（Leave）：交换机 GVRP 端口收到离开通告（Leave message）到将 VLAN 信息从端口移除的时间间隔。如过在离开计时器到期前收到加入通告（Join message），GVRP 保持端口的 VLAN 信息，否则清除端口 VLAN 信息。当端口收到离开通告，端口的 GVRP 状态变为离开（Leaving）；当离开计时器到期，端口的 GVRP 状态变为空（Empty）。离开计时器的取值范围从加入计时器的 3 倍到全部离开计时器的 1/5；默认值是 600 毫秒。
- 全部离开计时器（Leaveall）：GVRP 向所有 GVRP 端口发送全部离开通告（Leaveall messages)的最小时间间隔。全部离开通告采取使旧的 VLAN 信息老化，添加新的 VLAN 信息，从而保证了 VLAN 信息的准确性。全部离开通告使 GVRP 端口将端口状态变成离开（Leaving)，对于那些离开计时器到期前还没有收到加入通告的端口，清除其 VLAN 信息。全部离开计时器的默认值是 10000，一般将此计时器设置为离开计时器的 5 倍。

命令：　[no] join-timer <ms> leave-timer <ms> leaveall-timer <ms>

功能：　改变 GVRP 计时器

命令模式：　GVRP 配置模式

参数：　<ms>为各计时器的值

使用指南：　记时器的值的改变是以 100ms 为单位增减的；离开记时器的值必须大于或等于加入记时器的 3 的倍数；全部离开记时器的值必须大于或等于离开记时器的 5 的倍数；使用 GVRP 交换信息时，所有 GVRP 记时器的值的设置必须一致。

举例：

```
DCRS-7504(config-gvrp)#join timer-1000 leave-timer 3000 leaveall-timer 15000
```

该命令把 GVRP 的加入记时器值设为 1000、离开记时器值设为 3000、全部离开时间设为 15000。

命令：　default-timers

功能：　设置加入、离开、和全部离开的记时器为缺省值

命令模式：　GVRP 配置模式

使用指南：　该命令将计时器设置为如下值：

加入计时器：200 ms

离开计时器：600 ms
全部离开计时器：10000 ms

举例：

```
DCRS-7500(config-gvrp)# default-timers
```

#### 6.2.2.7 将 GVRP 生成的 VLAN 转换成静态 VLAN

用户不能改变 GVRP 生成的 VLAN 的参数，也无法将其保存在 running-config 和 startup-config 文件中。要想保存和配置 GVRP 生成的 VLAN，必须将 GVRP 端口转换成静态配置端口。

命令：　　[no] tagged ethernet <portnum> [to <portnum> | ethernet <portnum>]
功能：　　将 GVRP 生成的 VLAN 转换成静态 VLAN
命令模式：　GVRP 配置模式
参数：　　<portnum> [to <portnum> | ethernet <portnum>]指定太端口和以太端口范围
举例：

```
DCRS-7500(config)# vlan 22
DCRS-7500(config-vlan-22)# tagged ethernet 1/1 to 1/8
```

该命令把 GVRP 建立的 VLAN 转变成一个包括端口 E 1/1 到 E 1/8 的静态配置的 VLAN。

### 6.2.3 显示 GVRP 信息

用户可以显示下面的 GVRP 信息：

- GVRP 配置信息
- GVRP VLAN 信息
- GVRP 统计信息

#### 6.2.3.1 显示 GVRP 配置信息

命令：　　show gvrp [ethernet <port-num>]
功能：　　显示 GVRP 配置信息
命令模式：　全局配置模式
举例一：

```
DCRS-7504(config)#show gvrp
GVRP is enabled on the system

GVRP BASE  VLAN  ID              :4093
GVRP MAX  Leaveall   Timer          :300000  ms


GVRP Join Timer                     :200ms
```

```
GVRP Leave Timer                        :600 ms
GVRP Leave-all Timer                    :10000 ms

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - -
Configuration that is being used:
block-learning ethe 1/3
block-applicant ethe 2/7 ethe 2/11
enable ethe 1/1 to 1/7 ethe ethe 2/1 ethe 2/7 ethe 2/11

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - -
Spanning Tree :SINGLE SPANNING TREE
Dropped Packets Count: 0

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - -
Number of VLANs in the GVRP Database: 15
Maximum Number of VLANs that can be present: 4095

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - -
```

举例二：显示端口的 GVRP 配置信息

```
DCRS-7500(config)# show gvrp ethernet 2/1
Port 2/1 -
    GVRP Enabled    : YES
    GVRP Learning   : ALLOWED
    GVRP Applican   : ALLOWED
    Port State      : UP
    Forwarding      : YES
    VLAN Membership:        [VLAN-ID]           [MODE]
                                   1            FORBIDDEN
                                   2            FIXED
                                1001            NORMAL
                                1003            NORMAL
                                1004            NORMAL
                                1007            NORMAL
                                1009            NORMAL
                                1501            NORMAL
                                2507            NORMAL
                                4001            NORMAL
                                4093            FORBIDDEN
                                4094            FORBIDDEN
```

### 6.2.3.2 显示 GVRP VLAN 信息

命令： show gvrp vlan all | brief | <vlan-id>
功能： 显示 GVRP VLAN 信息
命令模式： 全局配置模式
参数： all 显示全部 GVRP VLAN 信息；brief 显示简要信息；<vlan-id>显示特定 VLAN 信息
举例一： 显示简要 GVRP VLAN 信息

```
DCRS-7504(config)#show gvrp vlan brief

Number of VLANs IN the GVRP Database: 7
Maximum Number of VLANs that can be present: 4095

[VLAN-ID]                    [MODE]                       [VLAN-INDEX]
1                            STATIC-DEFAULT                   0
7                            STATIC                           2
11                           STATIC                           4
1001                         STATIC                           7
1003                         DYNAMIC                          8
4093                         STATIC-GVRP-BASE-VLAN            6
4094                         IC-GVRP-BASE-VLAN                5
```

举例二： 显示指定 GVRP VLAN 信息

```
show gvrp vlan 1001

VLAN-ID: 1001,  VLAN-INDEX: 7,  STATIC: NO,     DEFAULT: NO,  BASE-VLAN: NO
Timer to Delete Entry Running: NO
Legend:[S-Slot]

Forbidden Members: None

Fixed Member: None

Normal(Dynamic) member:  (S2)   1
```

### 6.2.3.3 显示 GVRP 统计信息

命令： show gvrp statistics all | ethernet <port-num>
功能： 显示 GVRP 统计信息
命令模式： 全局配置模式
参数： all 显示全部 GVRP 统计信息；ethernet <port-num>显示端口 GVRP 统计信息

举例：

```
DCRS-7500(config)# show gvrp statistics ethernet 2/1
PORT 2/1 Statistics:
    Leave All Received                          : 147
    Join Empty Received                         : 4193
    Join In Received                            : 599
    Leave Empty Received                        : 0
    Leave In Received                           : 0
    Empty Received                              : 588
    Leave All Transmitted                       : 157
    Join Empty Transmitted                      : 1794
    Join In Transmitted                         : 598
    Leave Empty Transmitted                     : 0
    Leave In Transmitted                        : 0
    Empty Transmitted                           : 1248
    Invalid Messages/Attributes Skipped         : 0
    Failed Registrations                        : 0
```

#### 6.2.3.4 清除 GVRP 的统计信息

命令： clear gvrp statistics all | ethernet <portnum>
功能： 清除 GVRP 统计信息
命令模式： 全局配置模式
参数： all 清除全部 GVRP 统计信息；ethernet <port-num>清除端口 GVRP 统计信息
举例： DCRS-7500# clear gvrp statistics all

## 6.3 GVRP 配置举例

### 6.3.1 动态核心和固定边缘

在本例中边缘设备向核心设备通告静态配置 VLAN，核心设备从边缘设备学习 VLAN 信息而本身没有任何静态配置 VLAN。

在核心设备的配置如下：

```
DCRS-7500>enable
DCRS-7500#configure terminal
DCRS-7500(config)#gvrp-enable
DCRS-7500(config-gvrp)#enable all
```

这些命令全局地启用 GVRP 支持所有启用了该协议的端口

在边缘设备 A 上的配置如下：

```
DCRS-7500>enable
DCRS-7500#configure terminal
DCRS-7500(config)#vlan 20
DCRS-7500(config-vlan-20)#untagged 2/1
DCRS-7500(config-vlan-20)#tagged 4/24
DCRS-7500(config)#vlan 40
DCRS-7500(config-vlan-40)#untagged 2/1
DCRS-7500(config-vlan-40)#tagged 4/24
DCRS-7500(config-vlan-40)#exit
DCRS-7500(config)#gvrp-enable
DCRS-7500(config-gvrp)#enable ethernet 4/24
DCRS-7500(config-gvrp)#block-learning ethernet 4/24
```

这些命令的作用是：静态配置了两个基于端口的 VLAN(VLAN 20 和 VLAN 40)，在端口 4/24 上启用 GVRP，并且关闭该端口的学习功能。该设备能通告 VLAN 信息，但不能从其它设备学到 VLAN 信息。

在边缘设备 B 上的配置如下：

```
DCRS-7500>enable
DCRS-7500#configure terminal
DCRS-7500(config)#vlan 20
DCRS-7500(config-vlan-20)#untagged 2/24
DCRS-7500(config-vlan-20)#tagged 4/1
DCRS-7500(config)#vlan 30
DCRS-7500(config-vlan-30)#untagged 4/24
DCRS-7500(config-vlan-30)#tagged 4/1
DCRS-7500(config-vlan-30)#exit
DCRS-7500(config)#gvrp-enable
DCRS-7500(config-gvrp)#enable ethernet 4/1
DCRS-7500(config-gvrp)#block-learning ethernet 4/1
```

在边缘设备 C 上的配置如下：

```
DCRS-7500>enable
DCRS-7500#configure terminal
DCRS-7500(config)#vlan 30
DCRS-7500(config-vlan-30)#untagged 2/24
DCRS-7500(config-vlan-30)#tagged 4/1
DCRS-7500(config)#vlan 40
DCRS-7500(config-vlan-40)#untagged 4/24
DCRS-7500(config-vlan-40)#tagged 4/1
DCRS-7500(config-vlan-40)#exit
DCRS-7500(config)#gvrp-enable
DCRS-7500(config-gvrp)#enable ethernet 4/1
```

```
DCRS-7500(config-gvrp)#block-learning ethernet 4/1
```

### 6.3.2 动态核心和动态边缘

在这种配置方式下，核心设备和边缘设备没有被静态指定 VLAN，并且被启用通告和学习功能。边缘和核心设备去学习被配置在边缘网络上的 VLAN 信息。要启用所有端口的 GVRP 功能。

在边缘和核心设备上输入下面的命令：

```
DCRS-7500>enable
DCRS-7500#configure terminal
DCRS-7500(config)#gvrp-enable
DCRS-7500(config-gvrp)#enable all
```

### 6.3.3 固定核心和动态边缘

在这种配置方式下，边缘设备 GVRP 的学习功能是被启用的。核心设备上的 VLAN 是被静态配置的，并且核心设备被启用去通告其 VLAN 信息，但没有学习功能。边缘设备从核心设备学习 VLAN 的信息。

在核心设备上输入下面的命令：

```
DCRS-7500>enable
DCRS-7500#configure terminal
DCRS-7500(config)#vlan 20
DCRS-7500(config-vlan-20)#untagged 1/24
DCRS-7500(config-vlan-20)#tagged 6/24
DCRS-7500(config)#vlan 30
DCRS-7500(config-vlan-30)#tagged 6/24
DCRS-7500(config-vlan-30)#tagged 8/17
DCRS-7500(config)#vlan 40
DCRS-7500(config-vlan-40)#tagged 1/5
DCRS-7500(config-vlan-40)#tagged 8/17
DCRS-7500(config)#vlan 50
DCRS-7500(config-vlan-50)#untagged 6/1
DCRS-7500(config-vlan-50)#tagged 1/11
DCRS-7500(config-vlan-50)#exit
DCRS-7500(config)#gvrp-enable
DCRS-7500(config-gvrp)#enable ethernet 1/24 ethernet 6/24 ethernet 8/17
DCRS-7500(config-gvrp)#block-learning ethernet 1/24 ethernet 6/24 ethernet 8/17
```

这些 VLAN 命令配置 VLAN20，30，40 和 50。GVRP 命令启用连接到边缘设备的端口的 GVRP 协议，并且关闭了这些端口的 VLAN 学习功能。所有 VLAN 信息通过 GVRP 进行通告。

在边缘设备 A、B、C 上输入下面的命令：

```
DCRS-7500>enable
DCRS-7500#configure terminal
DCRS-7500(config)#gvrp-enable
DCRS-7500(config-gvrp)#enable all
DCRS-7500(config-gvrp)#block-applicant all
```

### 6.3.4 固定核心和固定边缘

在这种配置模式下，VLAN 被静态地配置在核心和边缘设备上。在每一个边缘设备上，VLAN 通告被启用，但是学习功能被关闭。GVRP 没有被配置到核心设备。这种配置启用边缘网络中的设备学习边缘设备的 VLAN。这种配置没有在核心设备上启用任何 GVRP 的功能。其配置与“动态核心和固定边缘”类似。

# 第7章 配置链路聚合（Trunk Groups）和动态链路聚合（Dynamic Link Aggregation）

## 7.1 链路聚合简介

本章介绍了如何配置链路聚合和 802.3ad 链路聚合。
- 链路聚合是手工配置多个端口的聚合链路
- 802.3ad 链路聚合是一种协议，能够动态创建和管理链路聚合

**注意**：同一交换机可以同时配置以上两种方式的链路聚合，但同一端口只能配置两种方式的一种。

链路聚合允许用户在两台交换机或一台交换机和一台服务器之间手工配置多条高速、负载分担的链路。用户可以配置 2 至 4 个端口作为一个链路聚合，支持高达双向 4 Gbps 的流量。

在 DCRS-7500 交换机上，用户可以在 2 个千兆以太网模块（Gigabit Ethernet modules）配置多至 8 个端口的多模块链路聚合。通过激活负载均衡功能，链路聚合还提供了链路失效时使用备用路径的冗余功能。

**注意**：一个链路聚合中的端口形成了一条逻辑链路。然而，一个链路聚合中的所有端口必须连接到另一端的同一个设备上。

链路聚合分 2 种模式：交换机链路聚合（Switch trunk group）和服务器链路聚合（Server trunk group）
- 交换机链路聚合：用于交换机和交换机相连
- 服务器链路聚合：用于交换机和服务器相连

链路聚合与服务器相连时，要实现链路聚合的终结，服务器必须或者安装多个网卡（NICs）。

### 7.1.1 链路聚合规则

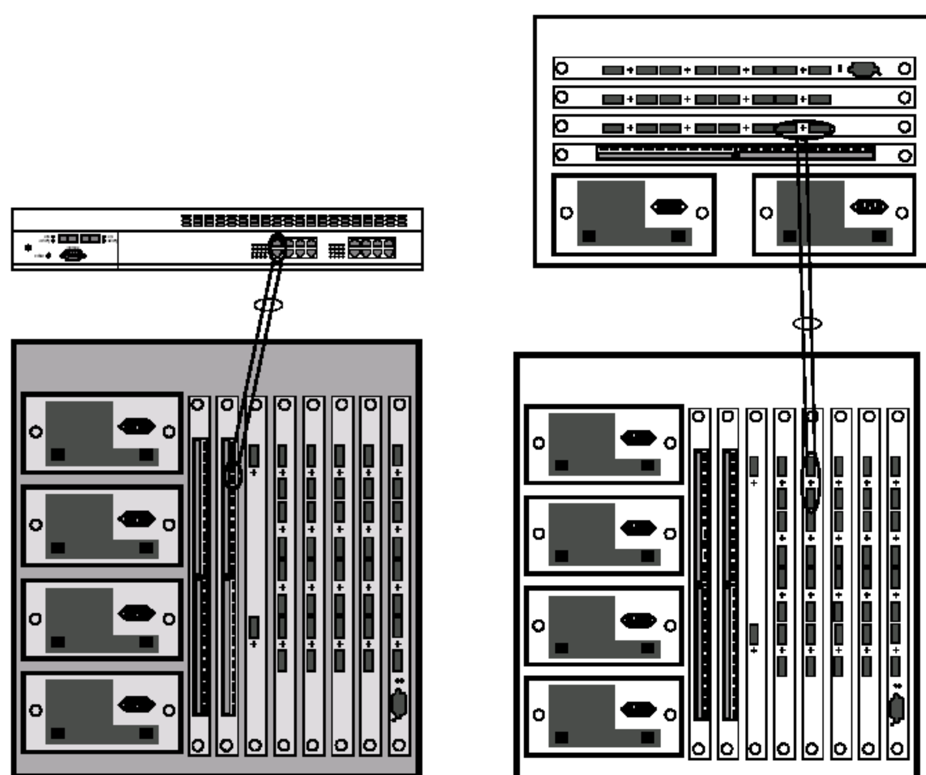
配置链路聚合必须遵照下列规则：
- 如果 802.3ad 链路聚合在一个端口被激活，这个端口不可以配置成链路聚合的成员
- 一个链路聚合最多可配置 8 个端口
- 每一个链路聚合必须从主端口（primary port）开始，主端口是下列端口范围的最小端口
  端口范围：1-4，5-8，9-12，13-16 ，17-18 和 21-24。对于千兆模块，主端口是 1,3,5 和 7
- 端口分配必须是连续的端口，不可有间隔
- 端口分配不能跨越多个链路聚合边界

- 一个链路聚合中的所有端口必须连接到另一端的同一个设备上
- 所有链路聚合成员的下列属性必须与组中主端口一致
  - 端口标签类型（tag type）
  - 端口速度和双工
  - QoS 优先级

  要改变端口属性，用户必须在主端口上进行配置，交换机会自动将变化复制到组内其他端口

图 7.1 显示了合法的 2 端口链路聚合，1 台交换机的 2 个合法端口连接到另 1 台交换机的 2 个合法端口上。同样的规则适用于 4 端口的链路聚合。

图 7.1：2 端口的链路聚合



## 7.1.2 跨模块链路聚合规则

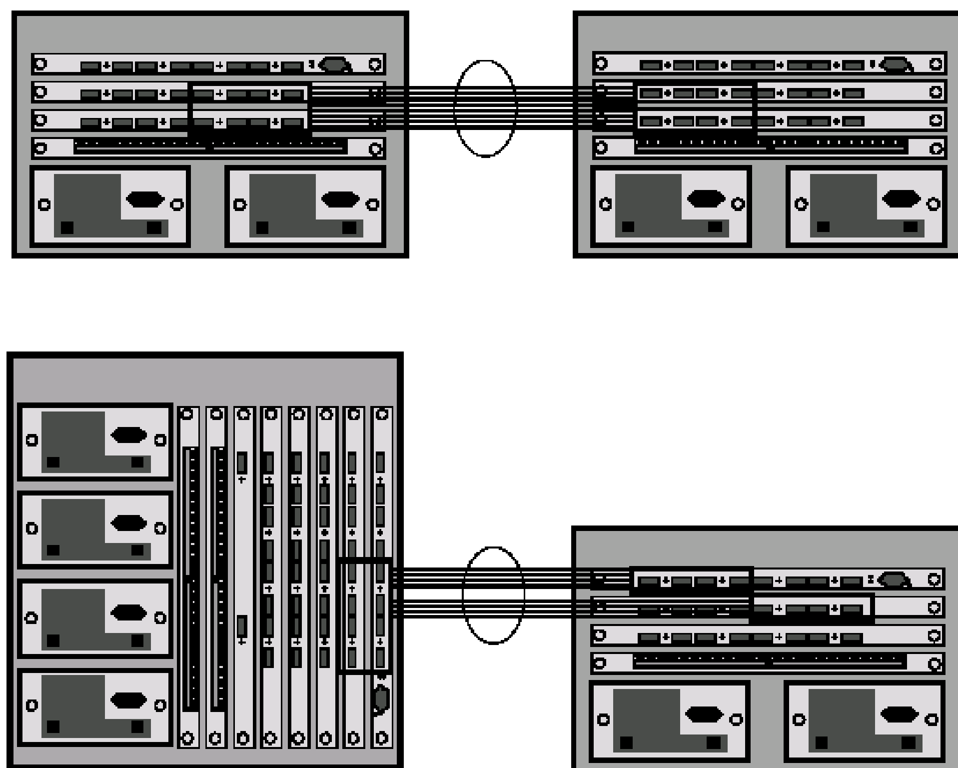
跨模块链路聚合除了要遵循 7.1.1 的规则外，还要遵循下列规则：

- 可以在 2 块千兆以太网模块上配置跨模块链路聚合
- 可以将 2 组链路聚合汇聚在一起形成新的链路聚合，但这 2 组链路聚合必须是相似的。比如，可以将 2 组 2 端口的链路聚合汇聚成新的链路聚合，但不能将 2 端口的链路聚合和 4 端口的链路聚合汇聚在一起。
- 当指定链路聚合的端口时，要以主端口开始，按升序排列。比如，必须按 1/1-1/4 and 3/1-3/4 来指定，不可以先指定 3/1-3/4。
- 当配置服务器链路聚合，要遵循下列规则：

- 服务器链路聚合所在模块和管理模块必须在同一插槽组中（插槽 1-7 或插槽 9-15），不要将他们安装在不同组中
- 不要将服务器链路聚合模块和管理模块安装在插槽 8 中

图 7.2 显示了 2 个交换机之间的跨模块链路聚合

图 7.2：跨模块链路聚合



## 7.2 配置链路聚合

### 7.2.1 配置步骤

按下列步骤配置链路聚合：

1. 将要配置链路聚合的端口的线缆拔下

注意：如果不拔下线缆直接在端口进行链路聚合配置，这些端口可能产生生成树环路

2. 配置链路聚合的2台交换机中的1台
3. 将配置文件保存在startup-config中
4. 在全局配置模式下输入命令“trunk deploy”链路聚合生效
5. 按照步骤2-4配置另一台交换机
6. 2台交换机都配置好后，重新连接链路聚合端口的线缆，连接时要先连接主端口的线缆
7. 使用命令“show trunk”命令检查运行状态

## 7.2.2 配置链路聚合举例

举例一：配置链路聚合

```
DCRS-7500(config)#trunk switch ethernet 8/1 to 8/8
Trunk will be created in next trunk deploy.
DCRS-7500(config)#write memory
.Write startup-config in progress.
.Write startup-config done.
DCRS-7500(config)#trunk deploy
```

上面命令将插槽 8 的以太网端口 1 至 8 做链路聚合。

命令：　　[no] trunk [server | switch] ethernet <primary-portnum> to <portnum>
功能：　　配置链路聚合
命令模式：　全局配置模式
参数：　　server | switch 表示交换机链路聚合或服务器链路聚合

举例二：配置跨模块链路聚合

```
DCRS-7500 (config)# trunk ethernet 1/1 to 1/2 ethernet 3/3 to 3/4
DCRS-7500 (config)# write memory
DCRS-7500 (config)# trunk deploy
```

命令：　　[no] trunk [server | switch] ethernet <primary-portnum> to <portnum> ethernet <primary-portnum> to <portnum>
功能：　　配置跨模块链路聚合
命令模式：　全局配置模式
参数：　　server | switch 表示交换机链路聚合或服务器链路聚合

## 7.2.3 其他配置命令

### 7.2.3.1　清除链路聚合

要清除链路聚合，只需在配置命令前加 no

举例：清除链路聚合

```
DCRS-7500 (config)# no trunk ethernet 1/1 to 1/2 ethernet 3/3 to 3/4
```

### 7.2.3.2 显示链路聚合状态

命令： show trunk [ethernet <portnum> to <portnum>]
功能： 显示链路聚合状态
命令模式： 特权配置模式
举例：

```
DCRS-7508(config)#show trunk ethernet 8/1 to 8/2

Configured trunks:

Trunk ID: 225
Type: Switch
Ports_Configured: 2
Primary Port Monitored: Jointly

Ports           8/1    8/2
Port Names      none   none
Port_Status     enable  enable
Monitor         off    off
Mirror Port     N/A    N/A
Monitor Dir     N/A    N/A

Operational trunks:

Trunk ID: 225
Type: Switch
Duplex: None
Speed: None
Tag: No
Priority: level0
Active Ports: 0

Ports           8/1    8/2
Link_Status     down    down
Load Sharing
 Mac Address        0       0
 IP             0       0
 IPX        0       0
 Apple Talk     0       0
 Multicast      0       0
```

## 7.3 动态链路聚合

神州数码 DCRS-7500 交换机支持 IEEE802.3ad 链路聚合。它使用 Link Aggregation Control Protocol (LACP)机制使冗余链路两端的端口自动配置链路聚合，而无需手工配置。当用户在一端交换机上配置动态链路聚合后，这些端口会自动与另一端的端口协商建立链路聚合。

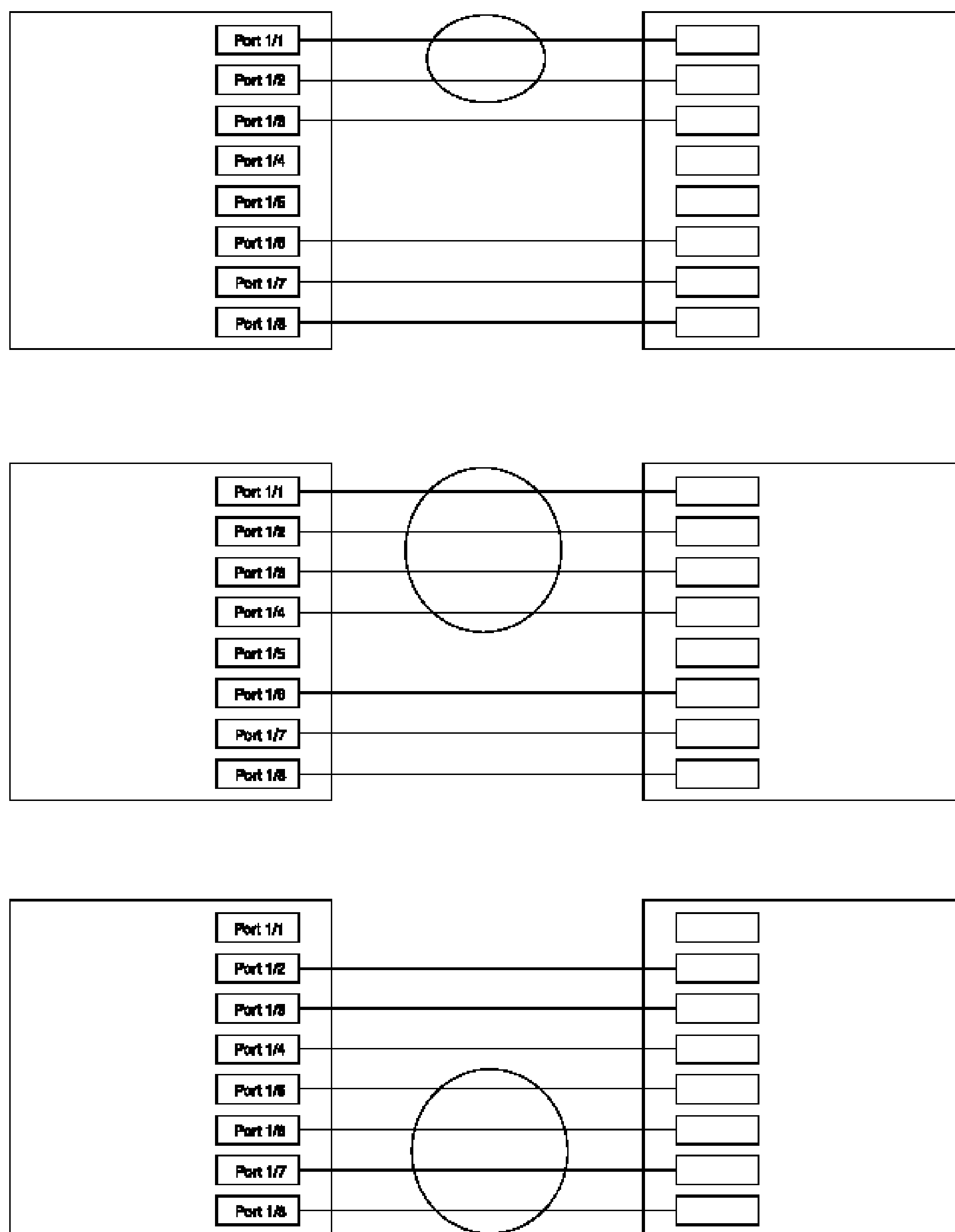
注意：

- 不能在已配置静态链路聚合的端口上配置 802.3ad 链路聚合
- 只能应用在 10/100/1000M 以太网接口
- 当 1 个端口作为第 2 个加入链路聚合组的端口，这个端口除了与链路聚合有关的配置外，其他的配置都被清除。例如，端口 1/3 有 IP 地址，当链路聚合功能将端口 1/3 加入端口 1/1 到端口 1/4 组成的链路聚合组时，端口 1/3 的 IP 地址被清除。
- 当交换机上运行 OSPF，动态链路改变会造成 OSPF 协议的重置。重置会造成 OSPF 短时中断，但很快会自动恢复正常运行

### 7.3.1 配置规则

动态链路聚合同样遵守静态链路聚合的配置规则。图 7.3 显示了一些合法的链路聚合。

图 7.3：合法链路聚合例子




在上面的例子中，假定左边神州数码 DCRS-7500 交换机和右边神州数码 DCRS-7500 交换机（或其他厂家交换机）上所有端口都配置了动态链路聚合，注意有一些端口并没有形成链路聚合，因为这些端口并不符合链路聚合的规则。动态链路聚合和静态链路聚合可以同时配置，它们的配置参数不相互妨碍。

**注意：**只有在另一端交换机支持 IEEE 802.3ad 链路聚合的时候才可以使用动态链路聚合；另一端交换机不支持的；需要手工配置。

默认状态下，动态链路聚合功能是关闭的。用户可以在端口上启用该功能，将其配置成

主动模式（active mode）或被动模式（passive mode）。

- 主动模式（active mode）：当动态链路聚合主动模式在端口上启用时，端口可以通过交换标准 LACP Protocol Data Unit (LACPDU)报文来同对端端口协商配置链路聚合。并且，端口主动发送 LACPDU 报文寻找对端链路聚合端口，之后发起 LACPDU 报文交换来协商链路聚合的参数。
- 被动模式（passive mode）：当动态链路聚合被动模式在端口上启用时，端口可以与对端端口交换 LACPDU 报文。但端口不能主动发送 LACPDU 报文寻找对端链路聚合端口，而必须依靠对端发起 LACPDU 报文交换。

## 7.3.2 开启动态链路聚合

默认状态下，动态链路聚合功能在所有端口关闭。

**命令：**　　[no] link-aggregate active | passive | off
**功能：**　　在端口上开启动态链路聚合功能
**命令模式：**　端口配置模式
**参数：**　　active 表示主动状态；passive 表示被动状态；off 表示关闭动态链路聚合功能
**举例一：**

```
DCRS-7500(config)# interface ethernet 1/1
DCRS-7500(config-if-e1000-1/1)# link-aggregate active
DCRS-7500(config)# interface ethernet 1/2
DCRS-7500(config-if-e1000-1/2)# link-aggregate active
```

上面命令将端口 1/1 和 1/2 配置成动态链路聚合的主动模式。

**举例二：**

```
DCRS-7500(config)# interface ethernet 1/5 to 1/8
DCRS-7500(config-mif-1/5-1/8)# link-aggregate passive
```

上面命令将端口 1/5 到 1/8 配置成动态链路聚合的被动模式。

## 7.3.3 配置动态链路聚合参数

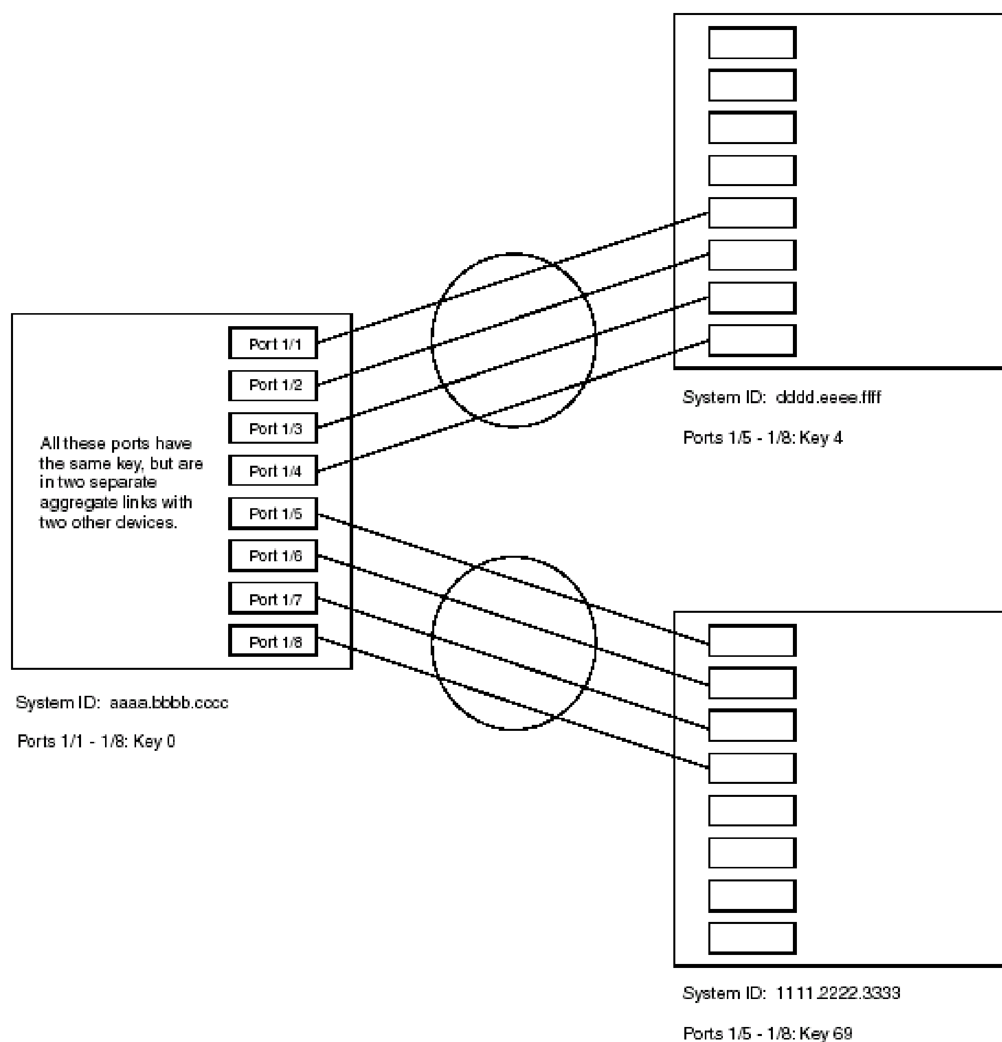
用户可以在端口上配置下列动态链路聚合参数：

- 系统优先级（System priority）：系统优先级定义了链路两端配置了动态链路聚合的交换机的优先级。优先级值越高优先级越低。优先级取值范围是 0-65535。默认值是 1。
- 端口优先级（Port priority）：端口优先级定义了端口的活动（active）和备用（standby）状态。当一台交换机上一组端口和另一台交换机上一组端口协商建立动态链路聚合，优先级较高的端口成为动态链路聚合的活动端口，其他端口成为动态链路聚合的备用端口。优先级值越高优先级越低。优先级取值范围是 0-65535。默认值是 1。
- 链路类型（Link type）：链路类型指定了链路聚合另一端是连接到服务器还是交换机。默认状态是交换机。
- 关键字（Key）：关键字定义了端口可以加入的链路聚合组。系统软件会自动根据端口 4

个一组的位置分配默认的关键字。关键字从 0 开始，按升序排列，分配从第 1 个 4 端口组开始。例如，1 个 8 端口的模块插在插槽 1 中，端口 1/1 到端口 1/4 的关键字是 0，端口 1/5 到端口 1/8 的关键字是 1。

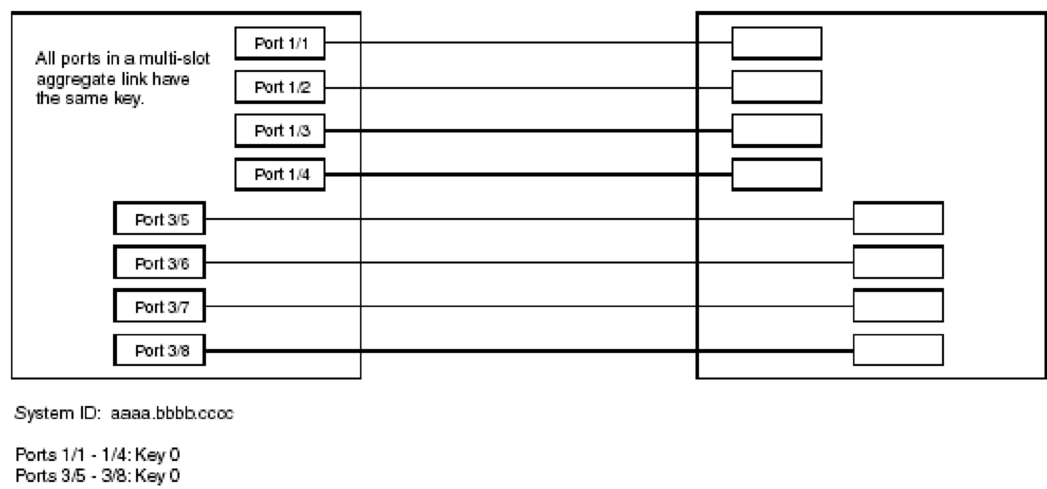
在同一个端口聚合组中的所有端口必须具有相同的关键字。允许 1 台交换机同时与 2 台交换机分别建立动态链路聚合，而这台交换机的 2 个链路聚合组拥有相同的关键字。图 7.4 显示了这样一个例子。

图 7.4：不同链路聚合组的端口具有相同关键字




当配置跨模块链路聚合是，所有模块上动态链路聚合的端口必须具有相同的关键字。例如，当配置端口 1/1 到端口 1/4 和端口 3/5 到端口 3/8 的链路聚合，所有 8 个端口的关键字必须一致。图 7.5 显示了这样一个例子：

图 7.5：跨端口链路聚合关键字




命令：　[no] link-aggregate configure [system-priority <num>] | [port-priority <num>] | [key <num>] | [type server | switch]

功能：　配置动态链路聚合参数

命令模式：　端口配置模式

参数：　system-priority <num>表示系统优先级；port-priority <num>表示端口优先级；key <num>表示关键字；type server | switch 表示链路类型

使用指南：　参数配置时顺序任意

举例：

```
DCRS-7500(config)# interface ethernet 1/1 to 1/4
DCRS-7500(config-mif-1/1-1/4)# link-aggregate configure key 10000
DCRS-7500(config-mif-1/1-1/4)# interface ethernet 3/5 to 3/8
DCRS-7500(config-mif-3/5-3/8)# link-aggregate configure key 10000
```

上述命令将端口 1/1 到端口 1/4 和端口 3/5 到端口 3/8 的关键字设置成 10000，这样上述端口可以配置跨模块动态链路聚合。

## 7.3.4 显示动态链路聚合信息

命令：　show link-aggregation [ethernet <portnum>]

功能：　显示动态链路聚合信息

命令模式：　任意模式

举例一：

```
DCRS-7500(config-mif-1/1-1/8)# show link-aggregation ethernet 1/1
System ID: 00e0.52a9.bb00
Port  [Sys P]  [Port P]  [ Key ]  [Act]  [Tio]  [Agg]  [Syn]  [Col]  [Dis]  [Def]
[Exp]
1/1      0        0          0       No    L     No      No    No     No      No
No
```

上述命令显示某一端口的动态链路聚合信息。

举例二：

```
DCRS-7500(config-mif-1/1-1/8)# show link-aggregation
System ID: 00e0.52a9.bb00
Port  [Sys P] [Port P] [Key] [Act] [Tio] [Agg] [Syn] [Col] [Dis] [Def] [Exp]
1/1    1       1        0     No    L     Agg   Syn   No    No    Def    Exp
1/2    1       1        0     No    L     Agg   Syn   No    No    Def    Exp
1/3    1       1        0     No    L     Agg   Syn   No    No    Def    Exp
1/4    1       1        0     No    L     Agg   Syn   No    No    Def    Exp
1/5    1       1        1     No    L     Agg   No    No    No    Def    Exp
1/6    1       1        1     No    L     Agg   No    No    No    Def    Exp
1/7    1       1        1     No    L     Agg   No    No    No    Def    Exp
1/8    1       1        1     No    L     Agg   No    No    No    Def    Exp
3/1    1       1        32    Yes   L     Agg   No    No    No    No     No
3/2    1       1        32    Yes   L     Agg   No    No    No    No     No
3/3    1       1        32    Yes   L     Agg   Syn   No    No    Def    Exp
3/4    1       1        32    Yes   L     Agg   Syn   No    No    Def    Exp
3/5    1       1        33    Yes   L     Agg   Syn   No    No    Def    Exp
3/6    1       1        33    Yes   L     Agg   Syn   No    No    Def    Exp
3/7    1       1        33    Yes   L     Agg   Syn   No    No    Def    Exp
3/8    1       1        33    Yes   L     Agg   Syn   No    No    Def    Exp
3/9    1       1        34    Yes   L     Agg   Syn   No    No    Def    Exp
3/10   1      1         34    Yes   L     Agg   Syn   No    No    Def    Exp
3/11   1       1        34    Yes   L     Agg   Syn   No    No    Def    Exp
3/12   1       1        34    Yes   L     Agg   Syn   No    No    Def    Exp
```

上述命令显示所有的动态链路聚合信息。

### **7.3.5** 清除协商的链路聚合配置

当动一组端口协商动态链路聚合时，系统软件将协商的配置保存在一个表中。用户可以清除这些协商的链路聚合配置。当清除这些配置时，并不清除链路聚合参数。

命令：　　clear link-aggregate

功能：　　清除协商的链路聚合配置

命令模式：　特权用户模式

举例：　　DCRS-7500# clear link-aggregate

# 第8章 安全功能的配置

## 8.1 MAC 地址端口验证

用户可以在 DCRS-7500 交换机的一个端口上配置有限数量的“安全”MAC 地址，这样交换机只转发源地址与安全 MAC 地址匹配的包。安全 MAC 地址可以手工配置或由交换机自动学习。当交换机学习到一个端口上指定数量的安全 MAC 地址后，对于该端口收到具有与安全 MAC 地址不同的源 MAC 地址的包视为非法。当发生非法行为时，Syslog 条目和 SNMP 陷阱会自动生成。并且，用户可以指定交换机执行下面两种操作中的一种：丢弃包含非法地址的包，或者将端口在指定的一段时间内关闭。

当端口被关闭又重新启动时，安全 MAC 地址不会丢失。这些 MAC 地址默认状态下会被永久保存，用户也可以配置超时时间（age out），使之在超时时间后不再是安全地址。用户还可以配置交换机在指定的时间间隔自动将安全地址列表保存在 startup-config 文件中，这样可以使安全地址在系统重启后仍然有效。

端口安全特性只适用于以太网接口。

端口安全使用本地或全局“资源”（resources）来决定每个接口可以有多少个安全 MAC 地址。“资源”是指存储安全 MAC 地址条目的能力。每个接口被分配 64 个本地资源。全局资源被交换机上所有的端口所共享，共有 2048 个。

当端口安全功能被启动时，端口可以存储 1 个安全 MAC 地址。用户可以利用本地资源将安全 MAC 地址的个数最多增至 64 个。

每个端口的最多安全 MAC 地址数是 64（最大本地资源）加上还没有被分配的全局地址数。

### 8.1.1 配置 MAC 地址端口验证

配置 MAC 地址端口验证需要执行下列操作：

- 开启 MAC 地址端口验证功能
- 设定端口最大安全 MAC 地址数量
- 设定 MAC 端口验证老化时间
- 设定安全 MAC 地址
- 配置交换机自动把安全 MAC 地址保存在 startup-config 文件中
- 指定违反安全规则的操作

#### 8.1.1.1 开启 MAC 地址端口验证功能

默认状态下，MAC 地址端口验证功能关闭，用户可以在全部端口或指定端口开启和关闭该功能。

命令： port security
功能： 配置 MAC 地址端口验证
命令模式： 全局配置模式或端口配置模式

命令： [no] enable
功能： 开启 MAC 地址端口验证功能
命令模式： MAC 地址端口验证模式
举例一：

```
DCRS-7500(config)# port security
DCRS-7500(config-port-security)# enable
```

上述命令在交换机全部端口上开启 MAC 地址端口验证功能。

举例二：

```
DCRS-7500(config)# int e 7/11
DCRS-7500(config-if-e100-7/11)# port security
DCRS-7500(config-port-security-e100-7/11)# enable
```

上述命令在交换机端口7/11上开启MAC地址端口验证功能。

#### 8.1.1.2 设定端口最大安全 MAC 地址数量

当 MAC 地址端口验证功能开启后，端口可以保存 1 个安全 MAC 地址。用户可以把这个值最大设置到 64 个。

命令： maximum <number-of-addresses>
功能： 设定端口最大安全 MAC 地址数量
命令模式： MAC 地址端口验证模式
参数： <number-of-addresses>指定最大安全 MAC 地址数量，取值范围从 1 到 64，默认值是 1。
举例：

```
DCRS-7500(config)# int e 7/11
DCRS-7500(config-if-e100-7/11)# port security
DCRS-7500(config-if-e100-7/11)# maximum 10
```

上述命令把端口 7/11 的最大安全 MAC 地址数量设定为 10。

#### 8.1.1.3 设定 MAC 端口验证老化时间

默认状态下，交换机学习的 MAC 地址在交换机中保存的时间不确定。用户可以配置安全 MAC 地址老化时间。

命令： [no] age <minutes>
功能： 设定 MAC 端口验证老化时间

命令模式：　MAC 地址端口验证模式
参数：　　　<minutes>设定 MAC 端口验证老化时间，以分钟为单位，默认是 0。
举例：

```
DCRS-7500(config)# int e 7/11
DCRS-7500(config-if-e100-7/11)# port security
DCRS-7500(config-port-security-e100-7/11)# age 10
```

上述命令把端口 7/11 的 MAC 端口验证老化时间设定为 10 分钟。

#### 8.1.1.4 设定安全 MAC 地址

命令：　　　[no] secure <mac-address>
功能：　　　设定安全 MAC 地址
命令模式：　MAC 地址端口验证模式
参数：　　　<mac-address>表示安全 MAC 地址。
举例：

```
DCRS-7500(config)# int e 7/11
DCRS-7500(config-if-e100-7/11)# port security
DCRS-7500(config-port-security-e100-7/11)# secure 0050.DA18.747C
```

上述命令在端口 7/11 上设定安全 MAC 地址 0050.DA18.747C。

#### 8.1.1.5 配置交换机自动把安全 MAC 地址保存在 startup-config 文件中

命令：　　　[no] autosave <minutes>
功能：　　　配置交换机自动把安全 MAC 地址保存在 startup-config 文件中
命令模式：　MAC 地址端口验证模式
参数：　　　<minutes>指定交换机自动把安全 MAC 地址保存在 startup-config 文件中的时间间隔。
举例：

```
DCRS-7500(config)# port security
DCRS-7500(config-port-security)# autosave 20
```

上述命令配置交换机每 20 分钟把安全 MAC 地址保存在 startup-config 文件中。

#### 8.1.1.6 指定违反安全规则的操作

当违反安全规则的情况发生时，例如：用户连接到交换机的端口，但 MAC 地址被锁定；或安全 MAC 地址超过最大数量，交换机会生成 SNMP trap 和 Syslog。

用户还可以配置交换机在发生违反安全规则时进行下列 2 种操作中的 1 种：丢弃所有非法地址的数据包或在一段时间内关闭端口。

命令：　　　violation restrict

功能： 违反安全规则时，丢弃所有非法地址的数据包

命令模式： MAC 地址端口验证模式

举例：

```
DCRS-7500(config)# int e 7/11
DCRS-7500(config-if-e100-7/11)# port security
DCRS-7500(config-port-security-e100-7/11)# violation restrict
```

上述命令配置交换机在端口 7/11 发生违反安全规则时，丢弃所有非法地址的数据包。

命令： violation shutdown <minutes>

功能： 违反安全规则时，在一段时间内关闭端口

命令模式： MAC 地址端口验证模式

参数： <minutes>指定交换机关闭端口的时间，取值范围是从 0 到 1440 分钟，当设定 0 时指违反安全规则时永远关闭端口。

举例：

```
DCRS-7500(config)# int e 7/11
DCRS-7500(config-if-e100-7/11)# port security
DCRS-7500(config-port-security-e100-7/11)# violation shutdown 5
```

上述命令配置交换机在端口 7/11 发生违反安全规则时，关闭端口 5 分钟。

## 8.1.2 显示 MAC 地址端口验证

用户可以显示下列 MAC 地址端口验证信息

- 显示存储在 startup-config 文件中的安全 MAC 地址
- 显示特定端口或模块上端口的 MAC 地址端口验证配置
- 显示交换机上配置的安全 MAC 地址
- 显示特定端口或模块上端口的 MAC 地址端口验证状态统计

### 8.1.2.1 显示存储在 startup-config 文件中的安全 MAC 地址

命令： show port security autosave

功能： 显示存储在 startup-config 文件中的安全 MAC 地址

命令模式： 特权配置模式

举例：

```
DCRS-7500# show port security autosave
```

### 8.1.2.2 显示特定端口或模块上端口的 MAC 地址端口验证配置

命令： show port security <module> | <portnum>

功能：　显示特定端口或模块上端口的 MAC 地址端口验证配置
命令模式：　特权配置模式
参数：　<module> | <portnum>指定模块或端口
举例：

```
DCRS-7500# show port security e 7/11
Port Security Violation Shutdown-Time Age-Time Max-MAC
----- -------- --------- ------------ --------- -------
7/11 disabled shutdown         10          10      1
```

上述命令显示端口 7/11 的 MAC 地址端口验证配置。

#### 8.1.2.3 显示交换机上配置的安全 MAC 地址

命令：　show port security mac
功能：　显示交换机上配置的安全 MAC 地址
命令模式：　全局配置模式
举例：

```
DCRS-7500(config)# show port security mac
Port Num-Addr Secure-Src-Addr Resource Age-Left Shutdown/Time-Left
----- -------- -------------- -------- --------- -----------------
7/11    1      0050.da18.747c   Local       10          no
```

#### 8.1.2.4 显示特定端口或模块上端口的 MAC 地址端口验证状态统计

命令：　show port security statistics <portnum>
功能：　显示特定端口的 MAC 地址端口验证状态统计
命令模式：　特权配置模式
参数：　<portnum>指定要显示的端口
举例：

```
DCRS-7500# show port security statistics e 7/11
Port Total-Addrs Maximum-Addrs Violation Shutdown/Time-Left
----- ----------- ------------ --------- -----------------
7/11      1              1          0           no
```

命令：　show port security statistics <module>
功能：　显示模块上端口的 MAC 地址端口验证状态统计
命令模式：　特权配置模式
参数：　<module>指定要显示的模块
举例：

```
DCRS-7500# show port security statistics 7
Module 7:
    Total ports: 0
```

```
Total MAC address(es): 0
Total violations: 0
Total shutdown ports 0
```

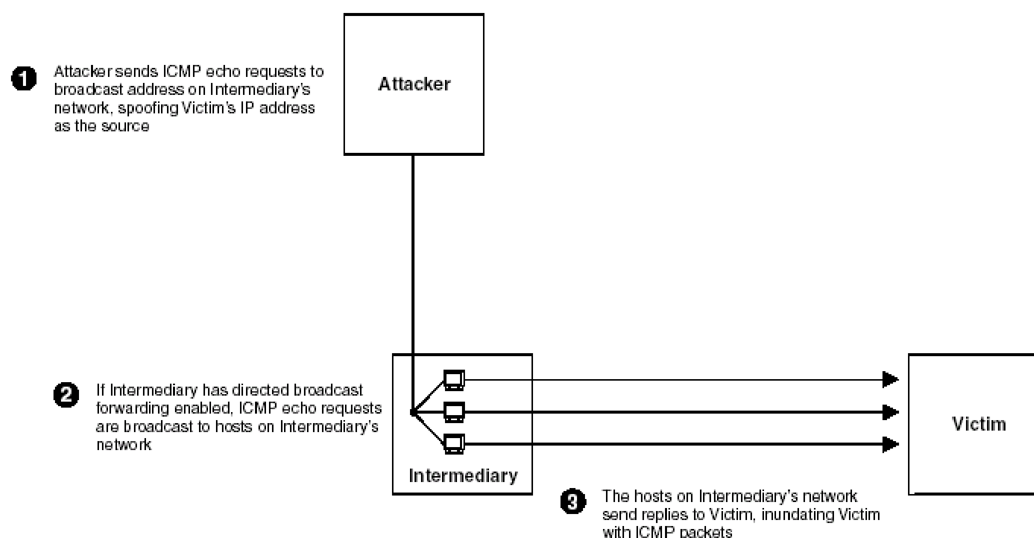
## 8.2 防止 DOS（Denial of Service）攻击

当发生 DoS 攻击时，路由器被无用的数据包淹没，无法正常工作。神州数码 DCRS-7500 交换机可以防范两种 DoS 攻击：Smurf 攻击和 TCP SYN 攻击

### 8.2.1 防范 Smurf 攻击

Smurf 攻击是 DoS 攻击的一种，攻击者使被攻击者被从其他网络发来的 ICMP（PING）回应包所淹没。图 8.1 演示了 Smurf 攻击的原理

图 8.1：Smurf 攻击的原理




攻击者向一个中间网络的广播地址发送 ICMP 请求包，这些 ICMP 请求包的源地址被伪造成被攻击者的地址。当 ICMP 请求包到达中间网络时，它们被转换成二层的广播地址，发送给中间网络的所有主机。然后，中间网络的主机会把 ICMP 回应包发送给被攻击者。攻击者每发送一个 ICMP 请求包，就会产生和中间网络中所有主机数量相等的 ICMP 回应包发送到被攻击者上。如果攻击者发送大量的 ICMP 请求包，而中间网络有大量的主机的话，被攻击者会被 ICMP 回应包淹没。

#### 8.2.1.1　防止成为 Smurf 攻击的中间媒介（Intermediary）

Smurf 攻击依靠中间媒介来向目标广播 ICMP 请求包。当 ICMP 请求包到达中间媒介时，

它们被转换成二层的广播地址，发送给中间网络的所有主机。也就是说，只有中间媒介允许对直接相连的网络传送广播信息，Smurf 攻击才会生效。

为了避免成为 Smurf 攻击的中间媒介，需要在交换机上关闭向直连的网络传送广播功能。

命令： [no] ip directed-broadcast
功能： 向直连网络传送广播
命令模式： 全局配置模式
举例：

```
DCRS-7500(config)# no ip directed-broadcast
```

#### 8.2.1.2 避免成为 Smurf 攻击的被攻击者

用户可以通过配置神州数码 DCRS-7500 交换机来防止其成为 Smurf 攻击的被攻击者。设置发送到交换机或交换机某一端口的 ICMP 包的阀值，当 ICMP 包的数量超过阀值时，丢弃 ICMP 包。

命令： ip icmp burst-normal <value> burst-max <value> lockup <seconds>
功能： 设置交换机接受 ICMP 包的阀值
命令模式： 全局配置模式
参数： burst-normal 值的范围是 1 – 100000
burst-max 值的范围是 1 – 100000
lockup 值的范围是 1 – 10000
使用指南： 此命令可在以太接口使用
举例一： 设置针对交换机的阀值：

```
DCRS-7500(config)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

举例二： 设置针对交换机端口的阀值

```
DCRS-7500(config)# int e 3/11
DCRS-7500(config-if-e100-3/11)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

每秒收到的 ICMP 包的数量按照如下规则与阀值进行比较：

- 当 ICMP 包的数量超过 burst-normal 值时，多出部分的 ICMP 包被丢弃
- 当 ICMP 包的数量超过 burst-max 值时，所有 ICMP 包在 lockup 值所指定的秒数内都被丢弃。lockup 抑制时间超时时，重新开始对 ICMP 包计数。

如上例所示，如果每秒收到的 ICMP 包超过 5000 个时，超出部分的包被丢弃。如果每秒收到的 ICMP 包超过 10000 个时，交换机在 300 秒内丢弃所有收到的 ICMP 包。

### 8.2.2 防范 TCP SYN 攻击：

TCP SYN 攻击通过干扰 TCP 连接建立的过程来达到中断网络流量的目的。当 TCP 连接启动时，源主机向目的主机发送 TCP SYN 包，目的主机回应 SYN ACK 包，源主机再向目的主机发送 ACK 确认包。这种机制被称为“TCP 三次握手”。

当目的主机等待源主机发送 ACK 确认包时，目的主机会建立未完成的 TCP 连接队列，当 ACK 确认包收到时，相关连接将从队列中移除。通常，目标主机回应 SYN ACK 包和源主机向目的主机发送 ACK 确认包之间不会间隔很长时间，所以连接队列很快会被清除。

当发生 TCP SYN 攻击时，攻击者发送大量的以随机产生的 IP 地址为源地址的 TCP SYN 包。对于每一个 TCP SYN 包，目的主机会回应 SYN ACK 包并将相关信息加入连接队列。由于源地址主机并不存在，所以目的主机不会收到任何 ACK 确认包。连接队列中的条目会在超时前保存在连接队列中（大约 1 分钟）。如果攻击者发送足够多的 TCP SYN 包，连接队列被占满，就会造成合法的 TCP 连接无法建立的情况。

为了防范 TCP SYN 攻击，用户可以设置发送到交换机或交换机某一端口的 TCP SYN 包的阀值，当 TCP SYN 包的数量超过阀值时，丢弃 TCP SYN 包。

**命令：** ip tcp burst-normal <value> burst-max <value> lockup <seconds>
**功能：** 设置交换机接受 TCP SYN 包的阀值
**命令模式：** 全局配置模式
**参数：** burst-normal 值的范围是 1 – 100000
burst-max 值的范围是 1 – 100000
lockup 值的范围是 1 – 10000
**使用指南：** 此命令可在以太接口使用
**举例一：** 设置针对交换机的阀值：

```
DCRS-7500(config)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

**举例二：** 设置针对交换机端口的阀值

```
DCRS-7500(config)# int e 3/11
DCRS-7500(config-if-e100-3/11)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

每秒收到的 TCP SYN 包的数量按照如下规则与阀值进行比较：

- 当 TCP SYN 包的数量超过 burst-normal 值时，多出部分的 TCP SYN 包被丢弃
- 当 TCP SYN 包的数量超过 burst-max 值时，所有 TCP SYN 包在 lockup 值所指定的秒数内都被丢弃。lockup 抑制时间超时时，重新开始对 TCP SYN 包计数。

如上例所示，如果每秒收到的 TCP SYN 包超过 10 个时，超出部分的包被丢弃。如果每秒收到的 TCP SYN 包超过 100 个时，交换机在 300 秒内丢弃所有收到的 TCP SYN 包。

### 8.2.3 显示因 DoS 攻击丢弃的数据包

显示因超出阀值丢弃的ICMP和TCP SYN数据包，使用下列命令。

命令：　show statistics dos-attack
功能：　显示因 DoS 攻击丢弃的数据包
命令模式：　全局配置模式
举例：
```
DCRS-7500(config)# clear statistics dos-attack
```

# 8.3 802.1x 端口验证

基于端口的验证，是由 IEEE 进行标准化的验证方法，标准号是 802.1x。IEEE 802.1x 定义了基于端口的网络接入控制协议(port based net access control)， 用于交换式的以太网环境，要求与客户和与其直接相连的设备都实现 802.1x。当应用于共享式以太网环境时，应对用户名、密码等关键信息进行加密传输。 在运营过程中，设备也可以随时要求客户重新进行验证。

该协议适用于接入设备与接入端口间点到点的连接方式，其中端口可以是物理端口，也可以是逻辑端口。主要功能是限制未授权设备（如用户计算机）通过以太网交换机的公共端口访问局域网。IEEE 802.1x 的体系结构包括三部分：

- Supplicant System 用户接入设备
- Authenticator System 接入控制单元
- Authentication Sever System 认证服务器

802.1x 系统的客户端一般安装在用户 PC 机中，典型为 Windows XP 的 802.1X 客户端。

接入层设备需要实现 802.1x 的认证系统部分，即 Authenticator。 主要根据客户的认证状态控制其物理接入，是客户与认证服务器之间的认证代理。

802.1x 的认证服务器系统（Authentication server）一般驻留在运营商的 AAA 中心，典型的是传统的 Radius 服务器。

接入层设备依据用户接入的端口状态决定该用户是否能接入网络。802.1x 系统将接入层设备端口分为非授权端口和授权端口。非授权端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证 Suppliant 始终可以发送或接收认证。授权端口只有在认证通过后才打开，用于传递网络资源和服务。授权端口双向授权、仅输入授权两种方式，以适应不同的应用环境。输入授权应用在集中桌面管理的应用场合，例如管理员即使在客户端关机的情况下也能通过授权端口向客户端发送远程开机命令。

在启用 802.1x 认证时，端口的初始状态一般为非授权状态（unauthorized），在该状态下，除 802.1x 报文和广播报文外不允许任何业务输入、输出。 当客户通过认证后，端口状态切换到授权状态，允许客户端通过端口进行正常通信。

接入层设备与客户端通过 EAPOL 协议进行通信，与认证服务器通过 EAPoRadius 或 EAP 承载在其他高层协议上进行通信。 接入层设备要求客户端提供 identity，接收到后将 EAP 报文承载在 Radius 格式的报文中，再发送到认证服务器，返回等同； 最后根据认证结果控制端口是否可用。认证服务器（Authentication server）核实客户的 identity，通知接入层设备是否允许客户端访问 LAN 和交换机提供的服务。

# 第9章 配置动态速率限制（Adaptive Rate Limiting）

神州数码 DCRS-7500 交换机提供动态速率限制功能。动态速率限制设定从 256 Kbps 到 1 Gbps，以 256 Kbps 为增量。用户可以在交换机上进行如下方式的速率设定：

- 基于端口（Port-based）：在端口上设定速率（bits per second）
- 基于端口和优先级（Port- and priority-based）：在端口上针对硬件转发队列设定速率
- 基于访问控制列表（ACL-based）：在端口上根据 IP 访问控制列表（IP Access Control Lists）设定速率。用户可以使用标准或扩展 IP 访问控制列表。标准访问控制列表根据 IP 源地址进行匹配，扩展访问控制列表根据源和目的地址进行匹配，对于 TCP 和 UDP，还要对 TCP 和 UDP 的源或目的地址进行匹配。交换机针对动态速率限制策略生成 CAM（Content Addressable Memory）表。CAM 表使交换机能够通过硬件进行动态速率限制而不必将流量发送到 CPU 进行处理。交换机将数据流（traffic flow）中的第一个包发送到 CPU，CPU 会生成针对这个数据流的 CAM 条目（entry）。一个数据流的条目包含数据的源和目的地址。交换机根据 CAM 条目对这个数据流进行动态速率限制。一个动态速率限制 CAM 条目被保存 2 分钟后超时。

注意：

- 不支持基于VLAN（VLAN-based）的动态速率限制
- 不支持基于VLAN和端口（Port-and-VLAN based）的动态速率限制
- 基于访问控制列表的动态速率限制只可在端口上配置，不能在虚拟路由接口（virtual routing interface）上配置。每端口可配置最多 10 条基于访问控制列表的动态速率限制策略；每交换机可配置最多 105 条基于访问控制列表的动态速率限制策略。不能将基于访问控制列表的动态速率限制应用在调节 IP 流量的 ToS 值。
- 基于端口的优先级的动态速率限制和基于访问控制列表的动态速率限制只支持入口（Inbound）动态速率限制策略
- 如果用户在同一端口配置动态速率限制和 ACL，动态速率限制不生效而只有 ACL 生效。

## 9.1 概览

**平均速率（Average Rate）**

平均速率是用户在配置动态速率限制策略时指定的一个参数。它表示某一端口线速（带宽）的百分比，以bps（bits per second）来表示。平均速率定义了每秒钟允许某一端口接受或发送的最大比特（bits）数，它取决于端口最大的线速以及用户所配置的入口（inbound）动态速率限制或出口（outbound）动态速率限制。Table 5.2 lists the minimum Average Rate for each traffic direction and port type. 端口最大平均速率是端口最大线速。

**调整的平均速率（Adjusted Average Rate）**

交换机软件调整用户指定的平均速率以避免产生不完整的“信用”（Credit）。CLI可以显示调整的平均速率。You also can display a table of the adjusted rate values. See “Displaying Adjusted Average Rates” on page 5-11. 对于出口的动态速率限制，端口需要

30至60秒转换成调整的平均速率。这种机制用于以下情况：

- 当在端口上应用出口动态速率限制策略时
- 当包的大小在段时间内变化很大时

“信用”（**Credit**）

“信用”是指限制速率端口的转发许可，还表示在一个动态速率限制时间间隔内可被转发的最小字节（bytes）数。入口动态速率限制“信用”是32字节；出口动态速率限制是64字节。在一个动态速率限制时间间隔内，一个端口只能接收或发送“信用”整倍数的字节。例如，一个端口的入口动态速率限制策略是一个动态速率限制时间间隔内接收或发送2个“信用”，那么这个端口在这个时间间隔内最多接收或发送64字节。

动态速率限制时间间隔（**Rate Limiting Interval**）

动态速率限制时间间隔定义了以毫秒为单位的动态速率限制的间隔。Table 5.2 lists the rate limiting interval Average Rate for each traffic direction and port type. JetCore芯片基于每个时间间隔来分配“信用”。

速率限制算法和参数

速率限制使用下面的算法

C = (R * I * 0.0000192) / (S * 8)

其中：

- C是“信用”的数量。C的值四舍五入。入口速率限制使用32字节信用；出口速率限制使用64字节信用。
- R是平均速率。它是1秒钟内允许通过的最大字节数。此参数可配置。
- I * 0.0000192的值是速率限制时间间隔。I的值取决于速率限制类型（入口或出口）和端口类型。见表9.1
- S是信用的长度。因为平均速率以位来表示，而信用以字节来表示，所以S的值需要乘8转换成位。

表9.1

| 流量形式 | 端口类型 | 最小平均速率(R) | 速率增量 | 时间间隔（I） | 信用长度 |
|---|---|---|---|---|---|
| 入口 | 10/100 | 256512 bps | 256512 bps | 52 | 32 |
| | Gigabit | 1025792 bps | 1025792 bps | 13 | 32 |
| 出口 | 10/100 | 1041910 bps | 41500 bps | 640 | 64 |
| | Gigabit | 20833792 bps | 833024 bps | 32 | 64 |

控制包的速率限制

对于基于端口和基于端口和优先级的模式，速率限制适用于所有包，包括控制包（control packets）。对于基于访问控制列表的模式，速率限制不适用于控制包。

配置注意事项

- 入口速率限制和出口速率限制是互不相关的。用户可以配置两者之一或同时配置两种；
- 对于出口速率限制，只支持基于端口的速率限制。不支持基于端口和优先级模式和基于

访问控制列表的模式；

➢ 对于入口速率限制，表9.2列出了可以同时使用的模式

表9.2：入口速率限制组合

| 速率限制类型 | 是否可被同时使用 | | |
|---|---|---|---|
| | 基于端口 | 基于端口和优先级 | 基于访问控制列表 |
| 基于端口 | | 不可以 | 可以 |
| 基于端口和优先级 | 不可以 | | 不可以 |
| 基于访问控制列表 | 可以 | 不可以 | |

# 9.2 配置动态速率限制

## 9.2.1 配置基于端口的速率限制

**命令：** [no] rate-limit in | out <average-rate>

**功能：** 在端口上限制速率

**命令模式：** 端口配置模式

**举例一：** 配置基于端口的入口速率限制

```
DCRS-7500(config)# interface ethernet 1/1
DCRS-7500(config-if-e100-1/1)# rate-limit in 600000
The average rate has been adjusted to 513024
```

上述命令在 10/100 端口 1/1 上将入口速率限制配置为 513024 bps。

**举例二：** 配置基于端口的出口速率限制

```
DCRS-7500(config)# interface ethernet 1/2
DCRS-7500(config-if-e100-1/2)# rate-limit out 5000000
The average rate has been adjusted to 5000192
```

上述命令在 10/100 端口 1/2 上将出口速率限制配置为 5000192 bps。

**举例三：** 配置基于千兆端口的出口速率限制

```
DCRS-7500(config)# interface ethernet 2/2
DCRS-7500(config-if-e1000-2/2)# rate-limit out 40000000
The average rate has been adjusted to 40000512
```

## 9.2.2 配置基于端口和优先级的速率限制

基于端口和优先级的速率限制只支持入口流量。

**命令：** [no] rate-limit in priority q0 | q1 | q2 | q3 <average-rate>

**功能：** 配置基于端口和优先级的速率限制

命令模式：　端口配置模式
使用指南：　此命令只应用于指定端口的指定硬件转发队列
举例：

```
DCRS-7500(config)# interface ethernet 1/1
DCRS-7500(config-if-e100-1/1)# rate-limit in priority q0 q2 600000
The average rate has been adjusted to 513024
```

上述命令把 10/100 端口 1/1 上的硬件转发队列 q0 和 q1 的出口速率限制配置为 5000192 bps。

### 9.2.3 配置基于访问控制列表的速率限制

用户可以使用标准或扩展访问控制列表进行速率限制。基于访问控制列表的速率限制只适用于入口流量。

命令：　[no] rate-limit in access-group <acl-id> <average-rate>
功能：　配置基于访问控制列表的速率限制
命令模式：　端口配置模式
使用指南：　必须先配置用于速率控制的访问控制列表
举例：

```
DCRS-7500(config)# access-list 50 permit host 1.1.1.2
DCRS-7500(config)# access-list 60 permit host 2.2.2.3
DCRS-7500(config)# interface ethernet 1/1
DCRS-7500(config-if-e100-1/1)# rate-limit in access-group 50 600000
The average rate has been adjusted to 513024
DCRS-7500(config-if-e100-1/1)# rate-limit in access-group 60 3000000
The average rate has been adjusted to 3077120
```

上述命令在10/100端口1/1配置了2个入口速率限制策略。第1个策略对从主机1.1.1.2发来的流量进行速率限制；第2个策略对从主机2.2.2.3发来的流量进行速率限制。

### 9.2.4 速率限制的语法

命令：　[no] rate-limit in | out [[priority q0 | q1 | q2 | q3] | [access-group <acl-id>]] <average-rate>
功能：　配置速率限制
命令模式：　端口配置模式
参数：　in | out 表示入口速率限制或出口速率限制
priority q0 | q1 | q2 | q3 表示适用于速率限制的端口硬件转发队列
access-group <acl-id> 表示适用于速率限制的访问控制列表
average-rate 表示允许端口每秒转发的最大位数，取值范围如下：
10/100 端口的入口速率限定：256512 – 100000000 bps
千兆端口的入口速率限定：1025792 – 1000000000 bps
10/100 端口的出口速率限定：1041910 – 100000000 bps
千兆端口的出口速率限定：20833792 – 1000000000 bps

## 9.3 显示动态速率配置信息

命令：　　　show rate-limit hardware-rate-limit-status
功能：　　　显示动态速率配置信息
命令模式：　任何模式
举例：

```
DCRS-7500(config-if-1/1)# show rate-limit hardware-rate-limit-status
*********************************************
*       Inbound JetCore Rate Limiting       *
*********************************************

Module: 1
  IPC number: 1
    Rate Limit Mode: Port Based
    Time Interval: 13*0.0192 (ms)
    Credit Size: 32
    Gig Enabled: Yes

    Port: 1/1, Rate: 3077120(bits/sec), Priority Queue: all, Dir: inbound, ACL: 
none
    Port: 1/2, Rate: 6153984(bits/sec), Priority Queue: all, Dir: inbound, ACL: 
none

  IPC number: 2
    Rate Limit Mode: Port Based
    Time Interval: 13*0.0192 (ms)
    Credit Size: 32
    Gig Enabled: Yes

    Port: 1/6, Rate: 6153984(bits/sec), Priority Queue: all, Dir: inbound, ACL: 
none
    Port: 1/2, Rate: 3077120(bits/sec), Priority Queue: all, Dir: inbound, ACL: 
none

Module: 2
  IPC number: 1
    Rate Limit Mode: Port Based
    Time Interval: 13*0.0192 (ms)
    Credit Size: 32
    Gig Enabled: Yes
```

```
   Port: 2/2, Rate: 3077120(bits/sec), Priority Queue: all, Dir: inbound, ACL:
none
   Port: 2/3, Rate: 3077120(bits/sec), Priority Queue: all, Dir: inbound, ACL:
none

  IPC number: 2
   Rate Limit Mode: Port Based
   Time Interval: 13*0.0192 (ms)
   Credit Size: 32
   Gig Enabled: Yes

   Port: 2/7, Rate: 6153984(bits/sec), Priority Queue: all, Dir: inbound, ACL:
none
   Port: 2/8, Rate: 6153984(bits/sec), Priority Queue: all, Dir: inbound, ACL:
none

*********************************************
*        Outbound JetCore Rate Limiting      *
*********************************************

Module: 1
   IPC number: 1
   Rate Limit Mode: Port Based
   Time Interval: 32*0.0192 (ms)
   Credit Size: 64
   Gig Enabled: Yes

   Port: 1/3, Rate: 30000128(bits/sec), Priority Queue: all, Dir: outbound, ACL:
none

   IPC number: 2
   Rate Limit Mode: Port Based
   Time Interval: 32*0.0192 (ms)
   Credit Size: 64
   Gig Enabled: Yes

   Port: 1/8, Rate: 60000256(bits/sec), Priority Queue: all, Dir: outbound, ACL:
   none
Module: 2
  IPC number: 1
    Rate Limit Mode: Port Based
    Time Interval: 32*0.0192 (ms)
    Credit Size: 64
    Gig Enabled: Yes
```

```
    Port: 2/2, Rate: 30000128(bits/sec), Priority Queue: all, Dir: outbound, ACL:
none
    Port: 2/3, Rate: 30000128(bits/sec), Priority Queue: all, Dir: outbound, ACL:
none

IPC number: 2
    Rate Limit Mode: Port Based
    Time Interval: 32*0.0192 (ms)
    Credit Size: 64
    Gig Enabled: Yes

    Port: 2/5, Rate: 30000128(bits/sec), Priority Queue: all, Dir: outbound, ACL:
none
```

# 第10章 配置基本三层功能

本章阐述如何在基本三层系统软件（Base Layer 3）上配置静态 IP 路由（static IP route）和 RIP。基本三层系统软件包括所有二层系统软件功能和下列功能：

- 置静态 IP 路由
- RIPv1 和 RIPv2
- 直连子网间路由
- 直连子网的 RIP 广播

本章主要阐述如何进行下列配置：

- 添加静态 IP 路由
- 在 ARP 表中添加静态条目
- 配置 RIP

## 10.1 添加静态 IP 路由

**命令：** [no] ip route <dest-ip-addr> <dest-mask> <next-hop-ip-addr> | null0 [<metric>]或
[no] ip route <dest-ip-addr>/<mask-bits> <next-hop-ip-addr> | null0 [<metric>]

**功能：** 添加静态 IP 路由

**命令模式：** 全局配置模式

**参数：** <dest-ip-addr>表示路由的目的地址；
<dest-mask>表示目的地址的网络掩码，也可以以“/”加上掩码的位数来表示，例如可以用 192.0.0.0/24 代替 192.0.0.0 255.255.255.0；
<next-hop-ip-addr>表示路由的下一跳路由器地址；
<metric>参数表示路由的代价，取值范围是 1 至 16，默认值是 1。Metric 是 RIP 使用的参数，如果没有激活 RIP，不需配置。

**使用指南：** 配置默认路由时，<dest-ip-addr>用 0.0.0.0 表示，<dest-mask>用 0.0.0.0 表示，<next-hop-ipaddr>用默认网关地址表示。

**举例：**

```
DCRS-7500(config)# ip route 209.157.2.0 255.255.255.0 192.168.2.1
```

上述命令添加了 1 条子网 209.157.2.x/24 的静态路由。

## 10.2 添加静态 ARP 条目

静态 ARP 条目使用户在没连接一台设备前预先配置好 ARP 映射条目，也可以用来防止特定的条目超时。一般情况下，1 条 ARP 条目在超时前没有收到更新信息时，系统软件会删除这个条目。而静态 ARP 条目一旦被创建则永远不会超时。

**命令：** [no] arp <num> <ip-addr> <mac-addr> ethernet <portnum> [vlan <vlan-id>]

**功能：** 添加静态 ARP 条目

**命令模式：** 全局配置模式

**参数：** <num>表示条目的编号。编号的范围是从 1 到交换机允许的最大值。用户可以把这个值最大设置到 1024，在全局配置模式下输入 **system-max ip-static-arp <num>**；
<ip-addr>表示 ARP 映射条目设备的 IP 地址；
<mac-addr>表示 ARP 条目的 MAC 地址；
ethernet <portnum>表示交换机连接具有 ARP 条目中 MAC 地址的设备的端口；
vlan <vlan-id>表示条目所属的基于端口的 VLAN 号码。当端口属于多个基于端口的 VLAN 时，必须指定次参数，否则不用指定。

**举例：**

```
DCRS-7500(config)# arp 1 209.157.22.3 aaaa.bbbb.cccc ethernet 3
```

上述命令添加 1 个 ARP 条目把 IP 地址 209.157.22.3 映射到 MAC 地址 aaaa.bbbb.cccc。MAC 地址连接的是 3 端口。

## 10.3 配置 RIP

默认状态下，RIP 是关闭的。配置 RIP 的过程是先全局开启该路由协议，再在端口上开启 RIP。当在端口上开启 RIP 时，还必须同时指定版本（version 1 only, version 2 only, 或 与 version 2 兼容的 version 1）。

### 10.3.1 开启 RIP

默认状态下，RIP 是关闭的。要开启 RIP，必须先全局开启，再在需要配置 RIP 的端口开启

**命令：** [no] router rip
**功能：** 开启 RIP
**命令模式：** 全局配置模式
**举例：**

```
DCRS-7500(config)# router rip
```

上述命令在全局开启 RIP。

**命令：** [no] ip rip v1-only | v1-compatible-v2 | v2-only
**功能：** 甚至 RIP 模式
**命令模式：** 端口配置模式
**举例：**

```
DCRS-7500(config-rip-router)# interface ethernet 1
DCRS-7500(config-if-1)# ip rip v1-only
```

上述命令在端口 1 开启 version 1 only 的 RIP 路由协议。

## 10.3.2 把 IP 静态路由再分配到 RIP 中

默认状态下，同软件不会把 IP 静态路由再分配到 RIP 中，要进行再分配，需要执行下列命令：

- 配置再分配过滤（可选）：用户可以根据路由的 metric 值允许或禁止再分配，也可以改变 metric 值。再分配过滤最多可以配置 64 条。系统软件使用升序来检查过滤条目，当有 1 条符合条件就立刻生效。比如第 1 条过滤禁止 1 条特定的路由再分配，即使序号较大的过滤条目允许该条路由的再分配，系统软件仍然不会再分配这条路由。

  **注意：**默认的再分配操作是允许所有再分配，所以如果要禁止某条路由再分配必须配置禁止过滤。
- 开启再分配

当用户开启路由再分配，默认状态下所有的 IP 静态路由都会被再分配。如果用户要禁止特定路由的再分配到 RIP 中，就需要配置禁止过滤，然后再开启再分配。

**命令：** [no] permit | deny redistribute <filter-num> static address <ip-addr> <ip-mask> [match-metric <value> | set-metric <value>]

**功能：** 配置再分配过滤

**命令模式：** RIP 路由配置模式

**参数：** <filter-num>表示再分配过滤编号，从 1 到 64；

address <ip-addr> <ip-mask>表示把再分配应用到特定的网络和子网。使用 0 表示“任何”，例如，“207.92.0.0 255.255.0.0”表示“任何 207.92.x.x 子网”。如果要指定任何子网，要使用“address 255.255.255.255 255.255.255.255”

match-metric <value>把再分配应用到具有特定 metric 值的路由，metric 值的范围是 1 到 15；

set-metric <value>给再分配到 RIP 的路由指定 RIP metric 值。

**举例一：**

```
DCRS-7500(config-rip-router)# deny redistribute 1 static address 207.92.0.0
255.255.0.0
```

上述命令禁止 IP 地址是 207.92.x.x 的静态路由再分配到 RIP。

**举例二：**

```
DCRS-7500(config-rip-router)# deny redistribute 2 static address 207.92.0.0
255.255.0.0 match-metric 5
```

上述命令禁止 IP 地址是 207.92.x.x 并且 metric 值是 5 的 IP 静态路由再分配到 RIP。

**举例三：**

```
DCRS-7500(config-rip-router)# deny redistribute 64 static address
255.255.255.255 255.255.255.255
DCRS-7500(config-rip-router)# permit redistribute 1 static address 10.10.10.0
255.255.255.0
DCRS-7500(config-rip-router)# permit redistribute 2 static address 20.20.20.0
255.255.255.0
```

上述命令禁止除 10.10.10.x 和 20.20.20.x 外的所有 IP 静态路由再分配到 RIP。

在配置完再分配过滤后，可以启动路由再分配。

**命令：** [no] redistribution
**功能：** 启动路由再分配
**命令模式：** RIP 路由配置模式
**举例：**

```
DCRS-7500(config-rip-router)# redistribution
```

上述命令启动路由再分配。

# 第11章 配置IP组播流量降低

默认状态下，神州数码 DCRS-7500 二层交换机根据数据包中的二层信息转发所有的 IP 数据流量。

用户可以配置 IP 组播流量降低（IP Multicast Traffic Reduction）特性使交换机进行基于硬件的 IP 组播组转发。当启用这项特性时，交换机会检查 IP 组播包中的 IP 组播地址，并只向收到该组播组成员报告（Group Membership reports）的端口转发数据。而对其他的组播组，交换机把数据转发到所有端口。

当启用 IP 组播流量降低特性时，用户可以同时配置下列特性：

- IGMP 模式（IGMP mode）：当用户启用 IP 组播流量降低特性时，二层交换机默认状态下被动侦听 IGMP 组成员报告（IGMP Group Membership report）。如果组播域中没有 1 台路由器发送 ICMP 询问（IGMP query）用以引发 IGMP 组成员报告，用户可以配置交换机主动发送 ICMP 询问。
- 询问间隔（Query interval）：询问间隔定义了二层交换机发送 ICMP 询问的时间间隔。询问间隔只应用于主动 IGMP 模式。其默认值是 60 秒，取值范围是从 10 到 600 秒。
- 老化时间：老化时间定义了 1 个 IGMP 组播组在没收到这个组的组成员报告前在 IGMP 组播组表中所保存的时间。如果二层交换机在收到新的这个组的组成员报告前，老化时间超时，交换机会从组播表中清除这个组的条目。默认老化时间是 140 秒。取值范围是从 10 到 1220 秒。
- 转发策略：二层交换机默认状态下转发所有 IP 组播流量。用户可以配置二层交换机使其只转发收到组成员报告的 IP 组播组，而丢弃其他组播组的流量。

## 11.1 启用 IP 组播流量降低（IP Multicast Traffic Reduction）

默认状态下，神州数码 DCRS-7500 二层交换机把 IP 组播流量转发到除接收端口外的所有端口。要降低通过二层交换机的流量，用户可以启用 IP 组播流量降低。这项功能使交换机只向连接组播组成员的端口转发组播流量。交换机根据 IGMP 表中的条目来判断端口是否连接组播组成员。每个条目包含 IP 组播组地址和交换机收到这个组播组组成员报告的端口号。

默认状态下，对于 IGMP 表中没有的条目，二层交换机会广播其流量。用户可以配置二层交换机过滤这些组的流量。详见？？？

用户启用 IP 组播流量降低后，当二层交换机收到发往 1 个 IP 组播组的流量后，交换机在 IGMP 表中查询这个组播组的条目。如果找到 1 个相符条目，交换机把组播流量转发到此条目所列的端口。如果没有找到任何相符条目，交换机广播组播流量。

IGMP 表由 IP 组播组成员发送的组成员通告生成。每个组成员通告包括组成员地址和组播组地址。二层交换机可以使用主动模式（active mode）或被动模式（passive mode）生

成 IGMP 表。默认状态下，二层交换机使用配动模式。

### 11.1.1 启用 IP 组播流量降低命令

命令：　　[no] ip multicast
功能：　　启用组播流量降低
命令模式：　全局配置模式
举例：

```
DCRS-7500(config)# ip multicast
```

上述命令在二层交换机上启用组播流量降低功能。

### 11.1.2 改变 IGMP 模式

当在二层交换机上启用 IP 组播流量降低功能时，也同时启用了 IGMP。交换机使用 IGMP 维护交换机所收到的组成员报告生成的表。用户可以使用主动或被动 IGMP 模式。默认状态下是被动状态。

- 主动状态：当启用主动 IGMP 模式时，二层交换机主动发送 IGMP 询问（IGMP query）来确认 IP 组播组和根据收到的组成员报告生成 IGMP 表中的条。

注意：通常网络中的路由器配置成主动状态。只有当交换机不和其他 IP 组播路由器相连时才可以使用主动模式。在这种情况下，只有 1 台交换机可以配置成主动模式，而其他交换机要配置成被动模式。

- 被动模式：当启用被动 IGMP 模式时，交换机侦听 IGMP 组成员报告，但不发送 IGMP 询问。被动模式有时被称为“IGMP 侦听”（IGMP snooping）。当网络中有其他设备主动发送询问时，交换机使用这种模式。

命令：　　[no] ip multicast active | passive
功能：　　改变 IGMP 模式
命令模式：　全局配置模式
举例一：

```
DCRS-7500(config)# ip multicast active
DCRS-7500(config)# write memory
DCRS-7500(config)# end
DCRS-7500# reload
```

上述命令启用主动 IGMP 模式。

举例二：

```
DCRS-7500(config)# ip multicast passive
DCRS-7500(config)# write memory
DCRS-7500(config)# end
DCRS-7500# reload
```

上述命令启用被动 IGMP 模式。

### 11.1.3 在端口上关闭 IGMP 功能

默认状态下，用户在二层交换机上启用 IP 组播功能时，交换机上所有端口都配置 IGMP。如果用户配置主动 IGMP 模式，所有端口都发送 IGMP 询问并接受 IGMP 报告。如果用户配置被动 IGMP 模式，所有端口接受 IGMP 询问。

如果想在端口上禁止所有 IP 组播流量，用户可以在相应端口上关闭 IGMP 功能。当用户关闭 1 个端口的 IGMP 功能时，交换机不会向这个端口转发任何组播流量，但其他端口仍然可以收发组播流量。

**命令：** [no] ip-multicast-disable
**功能：** 在端口上关闭 IGMP 功能
**命令模式：** 端口配置模式
**举例：**

```
DCRS-7500(config)# int e 1/5
DCRS-7500(config-if-1/5)# ip-multicast-disable
```

上述命令在端口 1/5 上关闭 IGMP 功能，但不影响其他端口的 IGMP 功能。

### 11.1.4 改变询问间隔

询问间隔定义了开启主动模式 IP 组播流量降低的二层交换机发送组成员询问的时间间隔。

**注意：**询问间隔只适用于主动模式的 IP 组播流量降低。

**命令：** [no] ip multicast query-interval <interval>
**功能：** 改变询问间隔
**命令模式：** 全局配置模式
**参数：** <interval>表示询问的时间间隔。默认时 60 秒，取值范围时 10 到 600 秒。
**举例：**

```
DCRS-7500(config)# ip multicast query-interval 120
```

上述命令把交换机发送询问的时间间隔定义为 120 秒。

### 11.1.5 改变老化时间

当收到组成员报告，交换机会在 IGMP 表中加入 1 条相关组的条目。老化时间定义了交换机收到新的组成员报告前，1 个条目在 IGMP 表中所能保存时间。

**命令：** [no] ip multicast age-interval <interval>
**功能：** 改变老化时间

**命令模式：** 全局配置模式

**参数：** <interval>表示老化时间。默认状态时 140 秒，取值范围是 10 到 1220 秒。

**举例：**

```
DCRS-7500(config)# ip multicast age-interval 280
```

上述命令把 IGMP 的老化时间改为 280 秒。

### 11.1.6 过滤组播组

默认状态下，交换机转发所有合法组播组的流量。用户可以配置二层交换机只转发收到组成员报告的组的流量，而过滤掉所有未收到组成员报告的组的流量。

配置过滤后，交换机启动后会转发所有组播组的流量。当收到 1 个组成员报告时，交换机会丢弃除这个组外所有其他组的流量。当收到其他组的组成员报告时，交换机开始停止丢弃相应组的流量，而转发其流量。

**命令：** [no] ip multicast filter

**功能：** 过滤组播组

**命令模式：** 全局配置模式

**举例：**

```
DCRS-7500(config)# ip multicast filter
```

上述命令使交换机开始过滤组播组。

## 11.2 PIM SM 流量侦听（PIM SM Traffic Snooping）

默认状态下，当二层交换机收到 IP 组播包时，它并不检查包中的组播信息而仅仅是简单的把组播包转发到除收到该包的端口外的所有端口。在一些网络中，这种方法会造成不必要的流量瓶颈。

例如，一台 DCRS-7500 二层交换机连接 1 个组播源和 2 个组播接收者，但每个端口都连接其他设备。尽管只有连接接收者的端口需要从组播源转发来的流量，但这台交换机会把组播流量转发到除连接组播源端口外的所有端口，这就增加了网络的负担。

PIM SM 流量侦听使二层交换机通过只向连接接收者的端口转发组播流量的方法来消除不必要的网络流量。

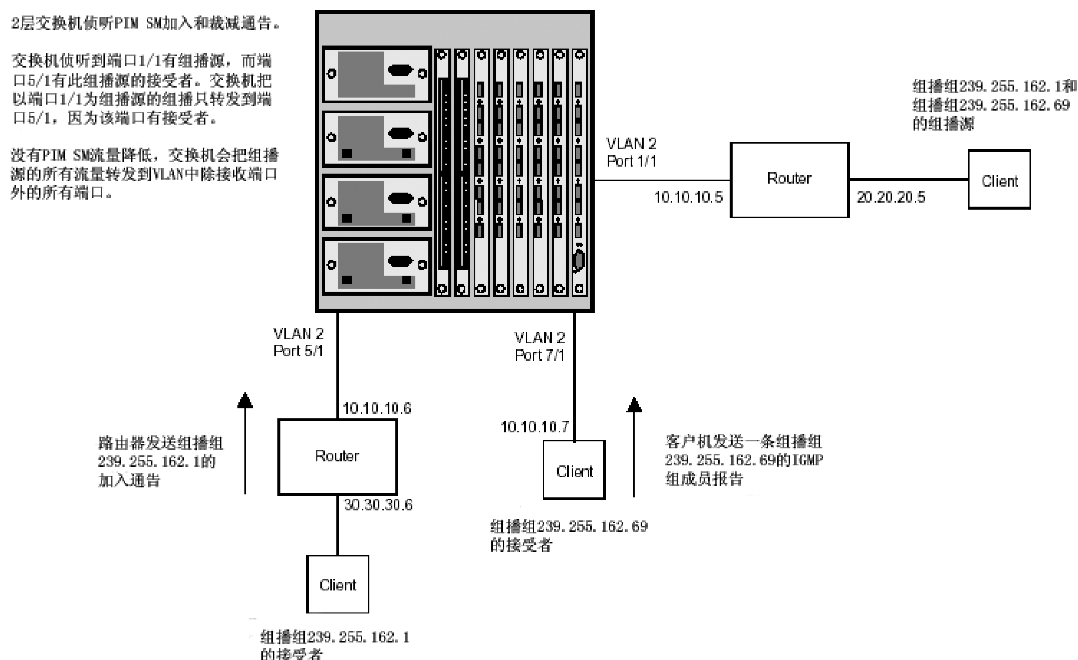
PIM SM 流量侦听需要开启 IP 组播流量降低功能。IP 组播流量降低功能使交换机侦听 IGMP 通告。PIM SM 流量侦听使交换机侦听 1 台 PIM SM 路由器发送给其他 PIM SM 路由器的 PIM SM 加入（join）和裁减（prune）通告来对组播流量进行更好的控制。

### 11.2.1 应用举例

图 11.1 是 1 个 PIM SM 流量侦听的举例。在这个例子里，二层交换机通过 1 台 IP 路由器连接到 1 个 PIM SM 组播源，这个组播源发送 2 个 PIM SM 组播组的流量。交换机同时

连接这 2 个组播组的 2 个接受者。

图 11.1：企业网的 PIM SM 流量降低




当开启 PIM SM 流量侦听后，二层交换机开始侦听 PIM SM 加入和裁减通告以及 IGMP 组成员报告。只有当二层交换机收到 1 个 PIM SM 加入通告或 IGMP 组成员报告时，交换机才开始把组播流量转发出所有端口。当交换机收到某 1 特定组播组的加入通告或组成员报告时，交换机会把所有后续的流量只转发到收到加入通告或 IGMP 组成员报告的端口。

在这个例子中，连接组播组 239.255.162.1 接收者的路由器向组播源发送 1 条加入通告。因为二层交换机上开启了 PIM SM 流量侦听，交换机会监测到加入通告，并生成 1 个条目包括组播组 ID 和连接接收者路由器的端口号码。当交换机下一次接收到从组播源 239.255.162.1 发出的流量时，交换机会把流量只转发到端口 5/1，因为只有这个端口连接 1 个接受者。

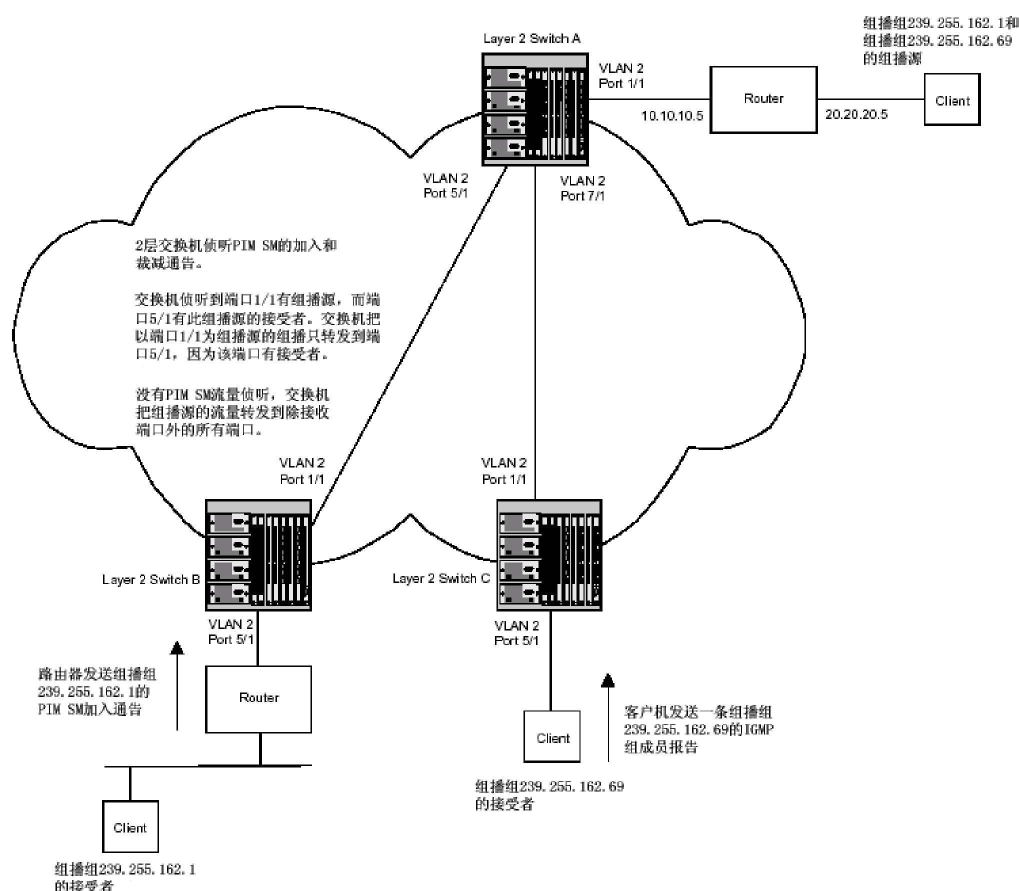
当组播组 239.255.162.69 的接收者直接连接到二层交换机上时，交换机无法收到客户端的加入通告。但是因为开启了 IP 组播流量降低，二层交换机通过客户端发出的 IGMP 组成员报告来选择通过哪一个端口转发组播组 239.255.162.69 的流量。PIM SM 流量侦听和 IP 组播流量降低一起建立了 VLAN 中的组播组和转发端口对应表。这个表包括从加入通告学习的 PIM SM 组播组和从 IGMP 组成员报告学习的 IP 组播组。在这个例子中，尽管二层交换机没有收到组播组 239.255.162.69 的加入通告，交换机仍然能够学习到接收者并把组播流量转发给接收者。

当端口收到某一组播组的裁减信息时，交换机停止向这个端口转发这一组播组的流量。

**注意：**PIM SM 流量侦听要求连接组播源和接收者的所有端口必须在同一个基于端口的 VLAN 中，而且要求组播源和下游的路由器在不同的 IP 子网中。参见图？？

图 11.2 是另一个 PIM SM 流量侦听的例子。这个例子显示了广域以太网云边缘的一些二层交换机。假设每一个二层交换机连接了大量的设备例如二层交换机和三层交换机（路由器）。

图 11.2：广域以太网环境的 PIM SM 流量侦听




广域以太网云边缘的二层交换机可以配置 IP 组播流量降低和 PIM SM 流量侦听。尽管需要配置多台二层交换机，但配置要求和 1 台二层交换机一样。

## 11.2.2 配置要求

- IP 组播流量降低必须同时被开启。PIM SM 流量侦听需要 IP 组播流量降低配合使用。

**注意：**应该使用被动模式的 IP 组播流量降低。被动模式假设路由器代表接收者发送组成员询问和加入、裁减通告。

- 二层交换机连接组播源和接收者（或连接接收者的路由器）的端口必须在同一基于端口的 VLAN 中。
- PIM SM 流量侦听功能假设组播源和二层交换机在不同的子网中，它们通过路由器进行通信。组播源和接收者也必须在不同 IP 子网中。只有当路由器和组播源在不同的子网中时，代表接收者的路由器才会发送 PIM 加入和裁减通告。如果接收者和组播源在同一子网中时，它们不需要路由器而可以直接发现对方。

  二层交换机默认会转发所有 IP 组播流量。当用户启用了 IP 组播流量降低和 PIM SM 流量侦听时，交换机会阻断所有组播流量。只有当交换机收到 1 条加入或裁减通告时，交换机才会开始转发 PIM SM 组播流量。这样，如果组播源和下游路由器在同一子网中，并且开启了 PIM SM 流量侦听时，交换机会阻断所有组播流量，永远不会开始转发。这是因为交换机永远不会收到下游路由器发送的加入和裁减通告，在同一子网中的下游路由器和组播组会直接发现对方而无需加入通告。

### 11.2.3 开启 PIM SM 流量侦听

要开启 PIM SM 流量侦听，必须先开启 IP 组播流量降低，再开启 PIM SM 流量侦听。

命令：　[no] ip pimsm-snooping

功能：　开启 PIM SM 流量侦听

命令模式：　全局配置模式

举例一：

```
DCRS-7500(config)# ip multicast passive
DCRS-7500(config)# ip pimsm-snooping
```

第一条命令开启 IP 组播流量降低功能。这项功能与 PIM SM 流量侦听功能相似，区别是它只侦听 IGMP 信息，不侦听 PIM SM 信息。用户必须开启 IP 组播流量降低和 PIM SM 流量侦听，这样交换机才能侦听 PIM SM 加入和裁减通告。另外 PIM SM 流量侦听功能假设网络中有路由器运行 PIM SM，所以交换机必须设为被动模式。

举例二：

```
DCRS-7500(config)# no ip pimsm-snooping
```

上述命令停止 PIM SM 流量侦听功能。

## 11.3 显示 IP 组播信息

### 11.3.1 显示一般信息

命令：　show ip multicast

功能：　显示一般组播信息

命令模式：　全局配置模式

举例：

```
DCRS-7500(config)# show ip multicast
IP multicast is enabled - Passive
VLAN ID 22
Active 5.5.5.1 Router Ports 3/4 3/10 5/3
Total number of Multicast Group: 1
    1 Multicast Group: 239.255.162.1, Port: 3/4 3/10 5/3
    IGMP Group Port:
    PIMv2 Group Port: 3/4 3/10 5/3
```

上述命令显示一般的组播信息，包括流量降低的状态和流量侦听的特性。

## 11.3.2 显示 PIM SM 组播信息

命令：　　show ip pim
功能：　　显示 PIM SM 组播信息
命令模式：全局配置模式
举例：

```
DCRS-7500(config)# show ip pim
PIMSM snooping is enabled
VLAN ID 22
PIMSM Neighbor list:
    5.5.5.2 : 3/4 expire 95 s
    5.5.5.3 : 3/10 expire 180 s
    5.5.5.1 : 5/3 expire 160 s
Multicast Group: 239.255.162.1, fid 000026bc camindex 2058
Forwarding Port: 3/4 3/10 5/3
PIMv2 Group Port: 3/4 3/10 5/3
(Source, Port) list:
    55.55.55.2, port: 3/10 5/3
    42.42.42.42, port: 3/4 3/10
    5.5.5.1, port: 3/10
    162.162.162.162, port: 3/4 5/3
```

上述命令显示了 PIM SM 组播的信息。

## 11.3.3 显示 IP 组播状态

命令：　　show ip multicast statistics
功能：　　显示 IP 组播状态
命令模式：全局配置模式
举例：

```
DCRS-7500# show ip multicast statistics
IP multicast is enabled - Passive

VLAN ID 1
Reports Received:                   34
Leaves Received:                    21
General Queries Received:           60
Group Specific Queries Received:    2
Others Received:                    0
General Queries Sent:               0
Group Specific Queries Sent:        0

VLAN ID 2
```

```
Reports Received:              0
Leaves Received:               0
General Queries Received:      60
Group Specific Queries Received:   2
Others Received:               0
General Queries Sent:          0
Group Specific Queries Sent:   0
```

上述命令显示了 2 个基于端口的 VLAN 的 IP 组播状态。

### 11.3.4 清除 IP 组播状态

命令： clear ip multicast statistics
功能： 清除 IP 组播状态
命令模式： 特权配置模式
举例：

```
DCRS-7500# clear ip multicast statistics
```

上述命令把所有 show ip multicast statistics 的命令所显示的参数状态设为 0。

### 11.3.5 清除所有 IGMP 组

命令： clear ip multicast all
功能： 清除所有 IGMP 组
命令模式： 特权配置模式
举例：

```
DCRS-7500# show ip multicast
IP multicast is enabled - Active
VLAN ID 1
Active 192.168.2.30 Router Ports 4/13
Multicast Group: 239.255.162.5, Port: 4/4 4/13
Multicast Group: 239.255.162.4, Port: 4/10 4/13

DCRS-7500# clear ip multicast all

DCRS-7500# show ip multicast
IP multicast is enabled - Active
VLAN ID 1
Active 192.168.2.30 Router Ports 4/13
```

上述命令可以看出 clear ip multicast all 清除了所有组播组。

## 11.3.6 清除特定 IGMP 组

命令：　　　clear ip multicast all | group <group-id>
功能：　　　清除特定 IGMP 组
命令模式：　特权配置模式
参数：　　　all 表示清除所有 IGMP 组；<group-id>表示清除特定的组播组。
举例：

```
DCRS-7500# show ip multicast
IP multicast is enabled - Active
VLAN ID 1
Active 192.168.2.30 Router Ports 4/13
Multicast Group: 239.255.162.5, Port: 4/4 4/13
Multicast Group: 239.255.162.4, Port: 4/10 4/13

DCRS-7500# clear ip multicast group 239.255.162.5

DCRS-7500# show ip multicast
IP multicast is enabled - Active
VLAN ID 1
Active 192.168.2.30 Router Ports 4/13
Multicast Group: 239.255.162.4, Port: 4/10 4/13
```

上述命令只清除了组播组 239.255.162.5。

# 第12章 升级系统文件及配置文件

本章阐述如何复制和保存系统文件和配置文件。

## 12.1 确认交换机上安装和运行的系统软件版本

使用下列方法显示交换机上运行的的系统软件版本和 Flash Memory 中安装的系统软件版本。

### 12.1.1 确认交换机上运行的 Flash 系统软件版本

确认交换机上运行的Flash系统软件版本，输入下列命令：

```
DCRS-7500# show version
SW: Version 07.1.05T51 Copyright (c) 1996-2001 Digitalchina Networks, Inc.
Compiled on Sep 29 2000 at 17:10:51 labeled as B2S07105
(1357024 bytes) from Primary b2s07105.bin
HW: Chassis 8000 Router, SYSIF version 21
==========================================================================
SL 2: Fiber Management Module, M3, ACTIVE
4096 KB BRAM, SMC version 1, ICBM version 21
512 KB PRAM(512K+0K) and 2048*8 CAM entries for DMA 4, version 0209
512 KB PRAM(512K+0K) and shared CAM entries for DMA 5, version 0209
512 KB PRAM(512K+0K) and 2048*8 CAM entries for DMA 6, version 0209
512 KB PRAM(512K+0K) and shared CAM entries for DMA 7, version 0209
==========================================================================
Active management module:
400 MHz Power PC processor 740 (version 8/8202) 66 MHz bus
512 KB boot flash memory
8192 KB code flash memory
256 KB SRAM
128 MB DRAM
The system uptime is 12 seconds
The system : started=warm start reloaded=by "reload"
```

上述输出结果中的黑体部分是版本信息：

- “**Version 07.1.05T51**”表示 Flash 系统软件版本。
- “**labeled as B2S07105**”表示 Flash 系统软件标注。这个标注显示了系统软件种类和版本，这些信息在用户改变系统文件名时尤其有用。
- “**Primary b2s07105.bin**”表示系统装载的系统文件名。

### 12.1.2 确认交换机上运行的启动文件（Boot Image）版本

确认交换机上运行的启动系统文件版本，，输入下列命令：

```
DCRS-7500> show flash
Active management module:
Code Flash Type: AMD 29F032B, Size: 64 * 65536 = 4194304, Unit: 2
Boot Flash Type: AMD 29F040, Size: 8 * 65536 = 524288
Compressed Pri Code size = 3265004, Version 07.5.00T53 (B2R07500.bin)
Compressed Sec Code size = 3620593, Version 07.2.06T53 (n2p0dm2.bin)
Maximum Code Image Size Supported: 3866112 (0x003afe00)
Boot Image size = 149436, Version 07.02.99 (bootrom.bin)
```

上述输出结果中的黑体部分是版本信息。

### 12.1.3 确认 Flash Memory 中安装的系统软件版本

输入 **show flash** 命令显示管理模块中安装的启动软件和系统软件。

- **"Compressed Pri Code size"**显示了安装在主 Flash 区（Primary Flash Area）的系统软件版本
- **"Compressed Sec Code size"**显示了安装在辅 Flash 区（Secondary Flash Area）的系统软件版本
- **"Boot Image size"** 显示了安装在 Flash Memory 中的启动软件版本。Flash Memory 中只有 1 个启动软件。

## 12.2 系统文件类型

表 12.1 列出神州数码 DCRS-7500 三层交换机支持的系统软件类型。

表 12.1：系统软件类型

| 产品 | 启动文件 | 系统软件 |
|---|---|---|
| DCRS-7515<br><br>DCRS-7508<br><br>DCRS-7504 | M2Bxxxxx.bin | ➢ D2Sxxxxx.bin (Layer 2 Switch code)<br>➢ DL3xxxxx.bin (Layer 2 Switch code with basic Layer 3 support)<br>➢ D2Rxxxxx.bin (Layer 3 Switch code) |

### 12.2.1 确认支持二层功能状态

要确认交换机支持二层交换的状态，在任何模式下输入下列命令：

```
DCRS-7500# show ip
Global Settings
ttl: 64, arp-age: 10, bootp-relay-max-hops: 4
router-id : 192.168.1.11
enabled : UDP-Broadcast-Forwarding Source-Route Load-Sharing RARP RIP
disabled: Route-Only Directed-Broadcast-Forwarding BGP4 IRDP Proxy-ARP RIP
-Redist OSPF DVMRP FSRP VRRP VRRP-Extended
```

如果“Route-Only”前是“enabled”，二层功能关闭；如果“Route-Only”前是“disabled”，二层功能开启。

## 12.3 升级系统软件

为了便于系统软件管理，神州数码 DCRS-7500 交换机支持交换机上的 Flash 模块和网络上的 Trivial File Transfer Protocol (TFTP)服务器之间进行系统软件的下载和上载。

交换机的管理模块包括 2 个 Flash Memory 模块：

- 主 Flash（Primary Flash)：交换机默认存储系统文件和配置文件的存储设备。
- 辅 Flash（Secondary Flash）:第 2 个 Flash 存储设备。可以保存备用的系统软件。

同一时刻只能有 1 个激活的 Flash 设备，默认状态下，主 Flash 在重启时被激活。

用户可以从 TFTP 服务器上载更新的系统软件到 Flash 模块中，也可以把 Flash 模块中的系统软件和配置文件复制到 TFTP 服务器上。

### 12.3.1 升级启动文件

使用下列方法升级启动文件：

1. 把更新的启动文件复制到 TFTP 服务器上，保证交换机可以访问 TFTP 服务器；
2. 在特权模式下输入下列命令之一，把 TFTP 服务器上的启动文件复制到 Flash 模块中
   - **copy tftp flash** <ip-addr> <image-file-name> **boot**
   - **ncopy tftp** <ip-addr> <image-file-name> **flash boot**
3. 在任何模式下输入下列命令，确认启动文件复制成功
   - **show flash**

   以“Boot Image size”开始的一行显示出启动文件的版本。
4. 如果启动文件的版本正确，输入下列命令之一重启使启动文件生效
   - **reload**（这条命令从默认系统文件，即主 Flash 启动）
   - **boot system flash primary** | **secondary**

### 12.3.2 升级系统软件

使用下列方法升级系统软件：

1. 更新的系统软件复制到 TFTP 服务器上，保证交换机可以访问 TFTP 服务器；
2. 在特权模式下输入下列命令之一，把 TFTP 服务器上的系统软件复制到 Flash 模块中
   - **copy tftp flash** <ip-addr> <image-file-name> **primary** | **secondary**
   - **ncopy tftp** <ip-addr> <image-file-name> **primary** | **secondary**
3. 在任何模式下输入下列命令，确认启动文件复制成功
   - **show flash**

   以"Compressed Pri Code size"开始的一行显示出主 Flash 中的系统软件的版本；同样以"Compressed Sec Code size" 开始的一行显示出辅 Flash 中的系统软件的版本
4. 如果系统软件的版本正确，输入下列命令之一重启使系统软件生效
   - **reload**（这条命令从默认系统文件即主 Flash 启动）
   - **boot system flash primary** | **secondary**

## 12.4 系统重启

用户可以使用boot命令从主Flash、辅Flash、BootP或者TFTP服务器重启交换机。

**注意**：务必在重启前检查是否成功地进行了TFTP传输。如果传输没有成功而用户重启交换机，交换机无法成功启动。

默认状态下三层交换机总是先尝试从主Flash启动交换机，再尝试从辅Flash启动交换机，最后尝试从TFTP服务器启动交换机。用户可以在全局配置模式下输入下列命令改变启动顺序：

- boot system bootp
- boot system flash primary
- boot system flash secondary
- boot system tftp

## 12.5 装载和保存配置文件

为了便于配置文件管理，神州数码DCRS-7500交换机支持交换机和网络上的TFTP服务器之间进行配置文件的下载和上载。用户可以把startup configuration或running configuration上载到TFTP服务器，用于备份或启动。

- Startup configuration file： 这个文件是存储于Flash中地配置文件。要显示这个文件，在任何模式下输入：show configuration
- Running configuration file：这个文件是当前系统运行的配置文件，它存储于系统的RAM中而非Flash中。要显示这个文件，在任何模式下输入命令“show running-config”或者命令“write terminal”

每台交换机只有1个Startup configuration file和1个Running configuration file。2个Flash模块共用1个Startup configuration file；Running configuration file存储于DRAM中。

### 12.5.1 用 Running Configuration 取代 Startup Configuration

更改系统配置后，用户可以把配置保存在Flash模块中，这实际上就是用Running Configuration取代Startup Configuration。

命令： write memory
功能： 把配置改变保存为 Flash 模块的 Startup Configuration
命令模式： 特权配置模式
举例：

```
DCRS-7500# write memory
```

上述命令把配置改变保存为Flash模块的Startup Configuration。

### 12.5.2 用 Startup Configuration 取代 Running Configuration

用户可以退出已做出的配置更改而使用Startup Configuration。

命令： reload
功能： 用 Startup Configuration 取代 Running Configuration
命令模式： 特权配置模式
举例：

```
DCRS-7500# reload
```

上述命令使交换机退出已做出的配置更改而使用Startup Configuration。

### 12.5.3 从 TFTP 服务器复制配置文件和把系统文件复制到 TFTP 服务器上

从 TFTP 服务器复制配置文件和把系统文件复制到 TFTP 服务器上，需要输入下列命令：

- copy startup-config tftp <tftp-ip-addr> <filename>：这条命令把交换机上的 Startup Configuration 上载到 TFTP 服务器上
- copy running-config tftp <tftp-ip-addr> <filename>：这条命令把交换机上的 Running Configuration 上载到 TFTP 服务器上
- copy tftp startup-config <tftp-ip-addr> <filename>：这条命令把 TFTP 服务器上的 Running Configuration 下载到交换机上

## 12.6 清除系统软件和配置文件

清除系统软件和配置文件，在特权模式下输入下列命令：

- erase flash primary：清除存储在主 Flash 中的系统文件
- erase flash secondary：清除存储在辅 Flash 中的系统文件
- erase startup-config：清除 Startup Configuration 文件，但 Running Configuration 文件会保留到下一次交换机重启